PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-288376

(43)Date of publication of application : 04.10.2002

(51)Int.Cl. G06F 17/60

(21)Application number : 2001-087300

(22)Date of filing : 26.03.2001

(71)Applicant : SANYO ELECTRIC CO LTD

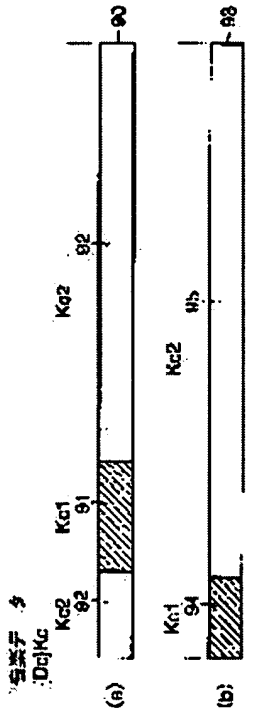
(72)Inventor : HORI YOSHIHIRO
HIOKI TOSHIAKI

(54) CONTENTS PROVIDING METHOD AND DATA REPRODUCING DEVICE AND DATA RECORDING DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a contents providing method for distributing enciphered contents data divided into a plurality of blocks and a plurality of licenses for decoding and reproducing the enciphered data included in those blocks.

SOLUTION: Enciphered contents data 90 or 93 obtained by enciphering music data are composed of trial enciphered music data 91 or 94 and main enciphered music data 92 or 95. The enciphered music data 91 and 94 are decoded by a license key Kc1, and the enciphered music data 92 and 95 are decoded by a license key Kc2. A distributing server holds the enciphered contents data 90 and 93 and the license keys Kc1 and Kc2, and distributes the trial enciphered music data 91 or 94 and the license key Kc1, and the main enciphered music data 92 or 95 and the license key Kc2 in this order in response to a distribution request.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of

rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）

(11)特許出願公開番号
特開2002－288376
（Ｐ２００２－２８８３７６Ａ）
(43)公開日　平成14年10月４日(2002.10.4)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
G06F 17/60	142	G06F 17/60	142	
	ZEC		ZEC	
	302		302 Ｅ	
	512		512	

審査請求　未請求　請求項の数13　ＯＬ　（全25頁）

(21)出願番号　特願2001－87300(Ｐ2001－87300)

(22)出願日　平成13年３月26日(2001.3.26)

(71)出願人　000001889
三洋電機株式会社
大阪府守口市京阪本通２丁目５番５号

(72)発明者　堀　吉宏
大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内

(72)発明者　日置　敏昭
大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内

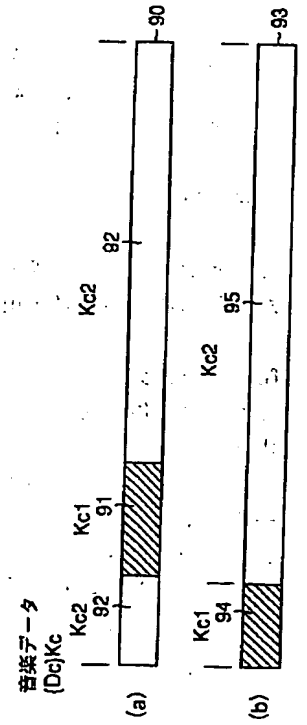
(74)代理人　100064746
弁理士　深見　久郎　（外３名）

(54)【発明の名称】コンテンツ提供方法、データ再生装置、およびデータ記録装置

(57)【要約】

【課題】　複数のブロックに分離された暗号化コンテンツデータと、複数のブロックに含まれる暗号化データを復号および再生するための複数のライセンスとを配信するコンテンツ提供方法を提供する。

【解決手段】　音楽データを暗号化した暗号化コンテンツデータ９０または９３は、試聴用の暗号化音楽データ９１または９４と本体用の暗号化音楽データ９２または９５から成る。暗号化音楽データ９１，９４はライセンス鍵Ｋｃ１によって復号され、暗号化音楽データ９２，９５はライセンス鍵Ｋｃ２によって復号される。配信サーバは、暗号化コンテンツデータ９０，９３およびライセンス鍵Ｋｃ１，Ｋｃ２を保持しており、配信要求に応じて試聴用の暗号化音楽データ９１または９４およびライセンス鍵Ｋｃ１、本体用の暗号化音楽データ９２または９５およびライセンス鍵Ｋｃ２の順序で配信する。



1

【特許請求の範囲】

【請求項１】　コンテンツデータを暗号化した暗号化コンテンツデータの取得要求を受信する第１のステップと、

前記第１のステップにおいて受信した取得要求に応じて、前記暗号化コンテンツデータを提供する第２のステップと、

前記暗号化コンテンツデータの一部に対応し、かつ、前記一部を復号するための第１のライセンスの提供要求を受信する第３のステップと、

前記第３のステップにおいて受信した提供要求に応じて、前記第１のライセンスを提供する第４のステップと、

前記第１のライセンスと異なり、かつ、前記暗号化コンテンツデータの前記第１のライセンスに対応しない他の一部に対応し、前記他の一部を復号するための第２のライセンスの提供要求を受信する第５のステップと、

前記第５のステップにおいて受信した提供要求に応じて、前記第２のライセンスを提供する第６のステップと、

前記第２のライセンスの提供に対して課金処理を行なう第７のステップとを含むコンテンツ提供方法。

【請求項２】　前記暗号化コンテンツデータ、前記第１のライセンス、および前記第２のライセンスが同じサーバから配信される、請求項１に記載のコンテンツ提供方法。

【請求項３】　前記暗号化コンテンツデータ、および前記第１のライセンスが第１のサーバから配信され、

前記第２のライセンスが前記第１のサーバと異なる第２のサーバから配信される、請求項１に記載のコンテンツ提供方法。

【請求項４】　前記暗号化コンテンツデータ、および前記第１のライセンスは、記録媒体を介して前記第１のサーバに供給される、請求項３に記載のコンテンツ提供方法。

【請求項５】　前記暗号化コンテンツデータが第１のサーバから提供され、

前記第１および第２のライセンスが前記第１のサーバと異なる第２のサーバから配信される、請求項１に記載のコンテンツ提供方法。

【請求項６】　前記暗号化コンテンツデータは、記録媒体を介して前記第１のサーバに供給される、請求項５に記載のコンテンツ提供方法。

【請求項７】　前記第３のステップにおいて、前記提供要求とともに認証データを受信し、前記認証データが認証されると前記第１のライセンスを提供し、

前記第５のステップにおいて、前記提供要求とともに認証データを受信し、前記認証データが認証されると前記第２のライセンスを提供する、請求項１から請求項６のいずれか１項に記載のコンテンツ提供方法。

2

【請求項８】　複数のブロックから成る暗号化コンテンツデータを前記複数のブロックに対応する複数のライセンスによって復号して再生するデータ再生装置であって、

前記暗号化コンテンツデータ、および前記複数のライセンスが記録されたデータ記録装置とのやり取りを行なうインタフェースと、

指示を入力するための操作部と、

前記暗号化コンテンツデータを前記複数のライセンスによって復号して再生するコンテンツ再生部と、

制御部とを備え、

前記制御部は、前記コンテンツ再生部において、前記暗号化コンテンツデータを構成するｎ番目（ｎは自然数）のブロックに含まれる暗号化データが前記ｎ番目のブロックに対応するｎ番目のライセンスによって復号および再生されているときに、ｎ＋１番目のライセンスを前記インタフェースを介して前記データ記録装置から取得して前記コンテンツ再生部に与える、データ再生装置。

【請求項９】　前記コンテンツ再生部は、

前記ｎ番目のライセンスに含まれるｎ番目のライセンス鍵を保持する第１のライセンス鍵保持部と、

前記ｎ＋１番目のライセンスに含まれるｎ＋１番目のライセンス鍵を保持する第２のライセンス鍵保持部と、

前記第１および第２のライセンス鍵保持部から前記ｎ番目のライセンス鍵と前記ｎ＋１番目のライセンス鍵とを選択的に取得し、その取得したライセンス鍵によって対応する暗号化データを復号する復号部と、

前記復号部によって復号されたコンテンツデータを再生する再生部とを含む、請求項８に記載のデータ再生装置。

【請求項１０】　前記制御部は、鍵変更情報を前記インタフェースを介して前記データ記録装置から取得し、前記鍵変更情報に基づいて前記ｎ番目のライセンス鍵と前記ｎ＋１番目のライセンス鍵とを選択して前記復号部に与える、請求項９に記載のデータ再生装置。

【請求項１１】　前記データ記録装置から前記複数のライセンスの各々を取得するセッションにおいて、異なるセッションキーを発生するセッションキー発生部と、

前記セッションキー発生部によって発生されたセッションキーを受け、そのセッションキーによって暗号化ライセンス鍵を復号し、その復号したライセンス鍵を前記第１または第２のライセンス鍵保持部に与えるライセンス鍵復号部とをさらに備え、

前記制御部は、前記セッションキー発生部によって発生されたセッションキーを前記インタフェースを介して前記データ記録装置に入力し、前記セッションキーによって暗号化された暗号化ライセンス鍵を前記インタフェースを介して前記データ記録装置から取得して前記ライセンス鍵復号部に与える、請求項１０に記載のデータ再生装置。

【請求項１２】　前記ライセンス鍵を提供するライセンス配信サーバから前記ライセンス鍵をダウンロードするための通信を行なうデータ送受信部をさらに備え、
前記制御部は、前記暗号化コンテンツデータの全部を再生するために必要なライセンスが前記データ記録装置に記録されていないとき、前記データ記録装置に格納されている前記暗号化コンテンツデータに対応する前記複数のライセンスによって再生可能なブロックのみを前記暗号化コンテンツデータの再生順に従って、前記データ記録装置から取得して前記コンテンツ再生部に与え、前記操作部から入力される新たなライセンス鍵の取得指示に従って前記ライセンス配信サーバから前記暗号化コンテンツデータを構成するブロックに対応するライセンス鍵を前記データ送受信部を介して受信し、その受信したライセンス鍵を前記データ記録装置に記録する、請求項８に記載のデータ再生装置。
【請求項１３】　複数のブロックから成る暗号化コンテンツデータおよび前記複数のブロックに含まれる複数の暗号化データを復号するための複数のライセンスとを記録するデータ記録装置であって、
前記複数のライセンスを格納するライセンス領域と、
前記暗号化コンテンツデータと、前記複数のライセンスの各々と前記暗号化コンテンツデータを構成する前記複数のブロックとの対応を示すライセンス対応情報とを格納するデータ領域とを備えるデータ記録装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、コピーされた情報に対する著作権保護を可能とするデータ配信システムにおけるコンテンツ提供方法、データ再生装置、およびデータ記録装置に関するものである。
【０００２】
【従来の技術】近年、インターネット等のデジタル情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。
【０００３】このようなデジタル情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。
【０００４】したがって、このようなデジタル情報通信網上において音楽データや画像データ等の著作者の権利が存在するコンテンツデータが伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。
【０００５】一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介してコンテンツデータの配信を行なうことができないとすると、基本的には、コンテンツデータの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【０００６】ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとって考えて見ると、通常販売されている音楽データを記録したＣＤ（コンパクトディスク）については、ＣＤから光磁気ディスク（ＭＤ等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やＭＤ等の媒体の代金のうちの一定額を間接的に著作権者に対して保証金として支払うことになっている。
【０００７】しかも、ＣＤからＭＤへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能なＭＤからさらに他のＭＤに音楽情報をデジタルデータとしてコピーすることは、著作権保護のために機器の構成上できないようになっている。
【０００８】このような事情からも、音楽データや画像データをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。
【０００９】この場合、デジタル情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。
【００１０】そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書を暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンス鍵を送信する。そして、暗号化コンテンツデータやライセンス鍵を配信する際、配信サーバおよびメモリカードは、配信毎に異なるセッションキーを発生させ、その発生させたセッションキーによって公開暗号鍵の暗号化を行ない、配信サーバ、メモリカード相互間で鍵の交換を行なう。
【００１１】最終的に、配信サーバは、メモリカード個々の公開暗号鍵によって暗号化され、さらにセッションキーによって暗号化したライセンスと、暗号化コンテン

5

ツデータとをメモリカードに送信する。そして、メモリカードは、受信したライセンスと暗号化コンテンツデータとを記録する。

【００１２】そして、メモリカードに記録された暗号化コンテンツデータを再生するときは、メモリカードを携帯電話機に装着する。携帯電話機は、通常の電話機能の他にメモリカードからの暗号化コンテンツデータを復号し、かつ、再生して外部へ出力するための専用回路も有する。

【００１３】このように、携帯電話機のユーザは、携帯電話機を用いて暗号化コンテンツデータを配信サーバから受信し、その暗号化コンテンツデータを再生することができる。

【００１４】暗号化コンテンツデータの配信においては、たとえば、音楽データを試聴用の暗号化音楽データと配信用の暗号化音楽データとに分離し、まず、試聴用の音楽データを配信し、ユーザが試聴用の音楽データを復号および再生して試聴した結果、配信用の暗号化音楽データとライセンスの配信を希望するときに配信用の暗号化音楽データとライセンスを配信することが行なわれている。このような場合、試聴用音楽データは本体用音楽データに比べて音質が劣っていて、仮に、試聴用音楽データをダウンロードしても著作権者の権利を損なわないようになっている。

【００１５】

【発明が解決しようとする課題】しかし、ユーザにとっては、試聴用音楽データによって購入しようとする音楽データの特定は可能であるが、提供される配信用音楽データの音質について確認できない。また、試聴用音楽データと配信用音楽データが同一である保証がない。

【００１６】このような、問題は音楽データに限らず、朗読データ、教材データ、ビデオデータ、ゲーム等のコンテンツデータの配信において同様に生じる。

【００１７】さらには、朗読データ、教材データ、ゲームなどのコンテンツデータにおいては、すべてのデータを一括で購入するのではなく、例えば、朗読データでは章ごとに、教材データやゲームなどではステージごとにユーザの配信要求に応じて配信する場合、複数回に分けて行なう配信に起因して、コンテンツデータの一括管理が難しくなるという問題が発生する。

【００１８】そこで、本発明は、かかる問題を解決するためになされたものであり、その目的は、複数の領域に分離された暗号化コンテンツデータと、複数の領域に含まれる暗号化データを復号および再生するための複数のライセンスとを配信するコンテンツ提供方法を提供することである。

【００１９】また、本発明の別の目的は、複数の領域に分離された暗号化コンテンツデータを複数のライセンスによって再生可能なデータ再生装置を提供することである。

6

【００２０】さらに、本発明の別の目的は、複数の領域に分離された暗号化コンテンツデータと複数のライセンスとを記録したデータ記録装置を提供することである。

【００２１】

【課題を解決するための手段】この発明によれば、コンテンツ提供方法は、コンテンツデータを暗号化した暗号化コンテンツデータの取得要求を受信する第１のステップと、第１のステップにおいて受信した取得要求に応じて、暗号化コンテンツデータを提供する第２のステップと、暗号化コンテンツデータの一部に対応し、かつ、一部を復号するための第１のライセンスの提供要求を受信する第３のステップと、第３のステップにおいて受信した提供要求に応じて、第１のライセンスを提供する第４のステップと、第１のライセンスと異なり、かつ、暗号化コンテンツデータの第１のライセンスに対応しない他の一部に対応し、他の一部を復号するための第２のライセンスの提供要求を受信する第５のステップと、第５のステップにおいて受信した提供要求に応じて、第２のライセンスを提供する第６のステップと、第２のライセンスの提供に対して課金処理を行なう第７のステップとを含む。

【００２２】好ましくは、暗号化コンテンツデータ、第１のライセンス、および第２のライセンスが同じサーバから配信される。

【００２３】好ましくは、暗号化コンテンツデータ、および第１のライセンスが第１のサーバから配信され、第２のライセンスが第１のサーバと異なる第２のサーバから配信される。

【００２４】好ましくは、暗号化コンテンツデータ、および第１のライセンスは、記録媒体を介して第１のサーバに供給される。

【００２５】好ましくは、暗号化コンテンツデータが第１のサーバから提供され、第１および第２のライセンスが第１のサーバと異なる第２のサーバから配信される。

【００２６】好ましくは、暗号化コンテンツデータは、記録媒体を介して第１のサーバに供給される。

【００２７】好ましくは、第３のステップにおいて、提供要求とともに認証データを受信し、認証データが認証されると第１のライセンスを提供し、第５のステップにおいて、提供要求とともに認証データを受信し、認証データが認証されると第２のライセンスを提供する。

【００２８】また、この発明によれば、データ再生装置は、複数のブロックから成る暗号化コンテンツデータを複数のブロックに対応する複数のライセンスによって復号して再生するデータ再生装置であって、暗号化コンテンツデータ、および複数のライセンスが記録されたデータ記録装置とのやり取りを行なうインタフェースと、指示を入力するための操作部と、暗号化コンテンツデータを複数のライセンスによって復号して再生するコンテンツ再生部と、制御部とを備え、制御部は、コンテンツ再

生部において、暗号化コンテンツデータを構成するｎ番目（ｎは自然数）のブロックに含まれる暗号化データがｎ番目のブロックに対応するｎ番目のライセンスによって復号および再生されているときに、ｎ＋１番目のライセンスをインタフェースを介してデータ記録装置から取得してコンテンツ再生部に与える。

【００２９】好ましくは、コンテンツ再生部は、ｎ番目のライセンスに含まれるｎ番目のライセンス鍵を保持する第１のライセンス鍵保持部と、ｎ＋１番目のライセンスに含まれるｎ＋１番目のライセンス鍵を保持する第２のライセンス鍵保持部と、第１および第２のライセンス鍵保持部からｎ番目のライセンス鍵とｎ＋１番目のライセンス鍵とを選択的に取得し、その取得したライセンス鍵によって対応する暗号化データを復号する復号部と、復号部によって復号されたコンテンツデータを再生する再生部とを含む。

【００３０】好ましくは、制御部は、鍵変更情報をインタフェースを介してデータ記録装置から取得し、鍵変更情報に基づいてｎ番目のライセンス鍵とｎ＋１番目のライセンス鍵とを選択して復号部に与える。

【００３１】好ましくは、データ記録装置から複数のライセンスの各々を取得するセッションにおいて、異なるセッションキーを発生するセッションキー発生部と、セッションキー発生部によって発生されたセッションキーを受け、そのセッションキーによって暗号化ライセンス鍵を復号し、その復号したライセンス鍵を第１または第２のライセンス鍵保持部に与えるライセンス鍵復号部とをさらに備え、制御部は、セッションキー発生部によって発生されたセッションキーをインタフェースを介してデータ記録装置に入力し、セッションキーによって暗号化された暗号化ライセンス鍵をインタフェースを介してデータ記録装置から取得してライセンス鍵復号部に与える。

【００３２】好ましくは、データ再生装置は、ライセンス鍵を提供するライセンス配信サーバからライセンス鍵をダウンロードするための通信を行なうデータ送受信部をさらに備え、制御部は、暗号化コンテンツデータの全部を再生するために必要なライセンスがデータ記録装置に記録されていないとき、データ記録装置に格納されている暗号化コンテンツデータに対応する複数のライセンスによって再生可能なブロックのみを暗号化コンテンツデータの再生順に従って、データ記録装置から取得してコンテンツ再生部に与え、操作部から入力される新たなライセンス鍵の取得指示に従ってライセンス配信サーバから暗号化コンテンツデータを構成するブロックに対応するライセンス鍵をデータ送受信部を介して受信し、その受信したライセンス鍵をデータ記録装置に記録する。

【００３３】また、この発明によれば、データ記録装置は、複数のブロックから成る暗号化コンテンツデータおよび複数のブロックに含まれる複数の暗号化データを復号するための複数のライセンスとを記録するデータ記録装置であって、複数のライセンスを格納するライセンス領域と、暗号化コンテンツデータと、複数のライセンスの各々と暗号化コンテンツデータを構成する複数のブロックとの対応を示すライセンス対応情報とを格納するデータ領域とを備える。

【００３４】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【００３５】図１は、本発明によるデータ記録装置が暗号化コンテンツデータを取得するデータ配信システムの全体構成を概念的に説明するための概略図である。

【００３６】なお、以下では携帯電話網を介してデジタル音楽データをユーザの携帯電話機に装着されたメモリカード１１０に、またはインターネットを介してデジタル音楽データをカードライタに装着されたメモリカード１１０に配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、動画像データ等を配信する場合においても適用することが可能なものである。

【００３７】図１を参照して、配信キャリア２０は、自己の携帯電話網を通じて得たユーザからの配信要求（配信リクエスト）を配信サーバ１０に中継する。著作権の存在する音楽データを管理する配信サーバ１０は、データ配信を求めてアクセスして来た携帯電話ユーザの携帯電話機１００に装着されたメモリカード１１０が正当な認証データを持つか否か、すなわち、コンテンツ保護機能を備えた正規のメモリカードであるか否かの認証処理を行ない、正規のメモリカードに対して暗号化コンテンツデータを復号するためのライセンスを配信する配信キャリア２０である携帯電話会社に、このような暗号化コンテンツデータおよびライセンスを与える。

【００３８】配信キャリア２０は、自己の携帯電話網を通じて配信要求を送信した携帯電話機１００に装着されたメモリカード１１０に対して、携帯電話網および携帯電話機１００を介して暗号化コンテンツデータとライセンスとを配信する。

【００３９】図１においては、たとえば携帯電話ユーザの携帯電話機１００には、着脱可能なメモリカード１１０が装着される構成となっている。メモリカード１１０は、携帯電話機１００により受信された暗号化コンテンツデータを受取り、上記配信にあたって行なわれた暗号化を復号した上で、携帯電話機１００中の音楽再生部（図示せず）に与える。

【００４０】さらに、たとえば携帯電話ユーザは、携帯電話機１００に接続したヘッドホーン１３０等を介してこのようなコンテンツデータを「再生」して、聴取する

ことが可能である。

【００４１】このような構成とすることで、まず、メモリカード１１０を利用しないと、配信サーバ１０からコンテンツデータの配信を受けて、音楽を再生することが困難な構成となる。

【００４２】しかも、配信キャリア２０において、たとえば１曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、携帯電話ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア２０が携帯電話機の通話料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【００４３】図１に示すデータ配信システムにおいては、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃは、ライセンス鍵Ｋｃ１にて復号可能な暗号化を施された領域である試聴領域｛Ｄｃ１｝Ｋｃ１と、ライセンス鍵Ｋｃ２にて暗号化を施された本体領域｛Ｄｃ２｝Ｋｃ２とから成り、一つの暗号化コンテンツデータとして構成されている。したがって、試聴には、ライセンス鍵Ｋｃ１を含む試聴用ライセンスが必要であり、コンテンツ全体の再生には、試聴用ライセンスとライセンス鍵Ｋｃ２を含む本体用ライセンスとが必要である。

【００４４】配信サーバ１０は、まず、携帯電話網を介して、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと、ライセンス鍵Ｋｃ１を含む試聴用ライセンスを携帯電話機１００へ配信する。そして、ユーザは、携帯電話機１００に備えられたコンテンツ再生回路（図示せず）において、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃの一部である試聴領域｛Ｄｃ１｝Ｋｃ１が試聴用ライセンスのライセンス鍵Ｋｃ１によって復号され、再生された音楽を聴き、このコンテンツをダウンロードしたいと思うと、再度、配信サーバ１０に対して本体用ライセンスの配信要求を送信する。そして、配信サーバ１０は、受信した配信要求に応じてライセンス鍵Ｋｃ２を含む本体用ライセンスを携帯電話網を介して携帯電話機１００に配信する。

【００４５】そうすると、携帯電話機１００のコンテンツ再生回路は、試聴用ライセンスに含まれるライセンス鍵Ｋｃ１と本体用ライセンスに含まれるライセンス鍵Ｋｃ２を用いて暗号化コンテンツデータ｛Ｄｃ｝Ｋｃの全てを再生できるようになる。

【００４６】また、図１においては、配信サーバ１０は、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃ、およびライセンス鍵Ｋｃ１を含む試聴用ライセンスをインターネット網３０を介してパーソナルコンピュータ５０に配信する。そして、パーソナルコンピュータ５０は、ＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）ケーブル７０およびカードライタ８０を介して暗号化音楽データ｛Ｄｃ｝Ｋｃおよびライセンス鍵Ｋｃ１を含む試聴用ライセンスの配信要求を受け、カードライタ８０に装着されたメモリカード１１０の正当性を上述したのと同じ方法によって判断し、正規なメモリカードに暗号化音楽データ｛Ｄｃ｝Ｋｃおよびライセンス鍵Ｋｃ１を含む試聴用ライセンスを記録する。そして、メモリカード１１０は、カードライタ８０から抜かれ、携帯電話機１００に装着される。携帯電話機１００のユーザは、装着されたメモリカード１１０から暗号化音楽データ｛Ｄｃ｝Ｋｃおよびライセンス鍵Ｋｃ１を読出し、暗号化音楽データ｛Ｄｃ｝Ｋｃの一部であるライセンス鍵Ｋｃ１によって復号可能な領域｛Ｄｃ１｝Ｋｃ１を復号および再生して試聴する。そして、ユーザは、暗号化音楽データ｛Ｄｃ｝Ｋｃの全てを再生するためにライセンス鍵Ｋｃ２を含む本体用ライセンスのダウンロードを希望するとき、携帯電話網３０を介して配信サーバ１０へライセンス鍵Ｋｃ２を含む本体用ライセンスの配信要求を送信する。そうすると、配信サーバ１０は、再び、メモリカード１１０が正規のメモリカードであることを確認した上でライセンス鍵Ｋｃ２を含む本体用ライセンスを携帯電話網を介して携帯電話機１００へ配信する。そして、携帯電話機１００は、受信したライセンス鍵Ｋｃ２を含む本体用ライセンスをメモリカード１１０に記録する。ユーザは、携帯電話機１００を用いてメモリカード１１０に記録された暗号化音楽データ｛Ｄｃ｝Ｋｃの全体はライセンス鍵Ｋｃ１およびライセンス鍵Ｋｃ２を用いて復号して再生する。

【００４７】ＣＤ－ＲＯＭ６０は、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃの試聴領域｛Ｄｃ１｝Ｋｃ１を復号するためのライセンス鍵Ｋｃ１を含む試聴用ライセンスとが記録されている。パーソナルコンピュータ５０は、ＣＤ－ＲＯＭ６０から暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと、試聴用ライセンスとを読出す。そして、パーソナルコンピュータ５０は、カードライタ８０に装着されたメモリカード１１０の正当性をカードライタ８０およびＵＳＢケーブル７０を介して確認し、正規なメモリカードにライセンス鍵Ｋｃ１を含む試聴用ライセンスを記録する。そして、メモリカード１１０は、カードライタ８０から抜かれ、携帯電話機１００に装着される。携帯電話機１００のユーザは、装着されたメモリカード１１０から暗号化音楽データ｛Ｄｃ｝Ｋｃの一部である試聴領域｛Ｄｃ１｝Ｋｃ１およびライセンス鍵Ｋｃ１を読出し、暗号化音楽データ｛Ｄｃ｝Ｋｃの一部を復号および再生して試聴する。そして、ユーザは、ライセンス鍵Ｋｃ２を含む本体用ライセンスのダウンロードを希望するとき、携帯電話網３０を介して配信サーバ１０へライセンス鍵Ｋｃ２を含む本体用ライセンスの配信要求を送信する。

【００４８】そうすると、配信サーバ１０は、メモリカード１１０が正規のメモリカードであることを確認した上でライセンス鍵Ｋｃ２を含む本体用ライセンスを携帯電話網を介して携帯電話機１００へ配信する。そして、携帯電話機１００は受信したライセンス鍵Ｋｃ２をメモ

リカード１１０に記録する。ユーザは、携帯電話機１００を用いてメモリカード１１０に記録された暗号化音楽データ｛Ｄｃ｝Ｋｃ、ライセンス鍵Ｋｃ１およびライセンス鍵Ｋｃ２を読出して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃの全てを再生する。

【００４９】この時、ＣＤ－ＲＯＭ６０に記録されている試聴用ライセンスは暗号化された上で記録され、メモリカード１１０にライセンスを記録するための専用プログラムによってのみアクセスできるようになっている必要がある。ＣＤ－ＲＯＭ６０上のライセンスをそのまま複製しても暗号化コンテンツデータ｛Ｄｃ｝Ｋｃの再生に用いることができない。

【００５０】また、ＣＤ－ＲＯＭ６０は、暗号化音楽データ｛Ｄｃ｝Ｋｃのみが記録されている。パーソナルコンピュータ５０は、ＣＤ－ＲＯＭ６０から暗号化音楽データ｛Ｄｃ｝Ｋｃを読出す。そして、パーソナルコンピュータ５０は、カードライタ８０およびＵＳＢケーブル７０を介して暗号化音楽データ｛Ｄｃ｝Ｋｃをメモリカード１１０に記録する。そして、メモリカード１１０は、カードライタ８０から抜かれ、携帯電話機１００に装着される。携帯電話機１００のユーザは、装着されたメモリカード１１０に記録された暗号化音楽データ｛Ｄｃ｝Ｋｃに対する試聴用ライセンスの配信を携帯電話機網および配信キャリア２０を介して配信サーバ１０へ要求する。

【００５１】図１に示すデータ配信システムにおいては、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃは、ライセンス鍵Ｋｃ１にて復号可能な暗号化を施された領域である試聴領域｛Ｄｃ１｝Ｋｃ１と、ライセンス鍵Ｋｃ２にて暗号化を施された本体領域｛Ｄｃ２｝Ｋｃ２とから成り、一つの暗号化コンテンツデータとして構成されている。したがって、試聴には、ライセンス鍵Ｋｃ１を含む試聴用ライセンスが必要であり、コンテンツ全体の再生には、試聴用ライセンスと、ライセンス鍵Ｋｃ２を含む本体用ライセンスとが必要となる。

【００５２】配信サーバ１０は、まず、携帯電話網を介して、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと、ライセンス鍵Ｋｃ１を含む試聴用ライセンスを携帯電話機１００へ配信する。そして、ユーザは、携帯電話機１００に備えられたコンテンツ再生回路（図示せず）において、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃの一部である試聴用領域｛Ｄｃ１｝Ｋｃ１が試聴用ライセンスのライセンス鍵Ｋｃ１によって復号され、かつ、再生された音楽を聴き、このコンテンツをダウンロードしたいと思うと、再度、配信サーバ１０に対して本体用ライセンスの配信要求を送信する。そして、配信サーバ１０は、受信した配信要求に応じてライセンス鍵Ｋｃ２を含む本体用ライセンスを携帯電話網を介して携帯電話機１００に配信する。

【００５３】そうすると、携帯電話機１００のコンテンツ再生回路は、試聴用ライセンスに含まれるライセンス鍵Ｋｃ１と本体用ライセンスに含まれるＫｃ２を用いて暗号化コンテンツデータ｛Ｄｃ｝Ｋｃのすべてを再生できるようになる。

【００５４】また、説明は省略するが、試聴用ライセンスと同様に本体用ライセンスもパーソナルコンピュータ５０がインターネット網３０を介して取得してメモリカード１１０に記録させることもできる。インターネット網３０を介してパーソナルコンピュータ５０に試聴用ライセンスまたは本体用ライセンスを配信する場合は、暗号通信を用いる。

【００５５】このように、メモリカード１１０は、各種の方法によって暗号化音楽データ｛Ｄｃ｝Ｋｃ、ライセンス鍵Ｋｃ１を含む試聴用ライセンスおよびライセンス鍵Ｋｃ２を含む本体用ライセンスを取得する。

【００５６】図１に示したような構成においては、暗号化して配信されるコンテンツデータを携帯電話機のユーザ側で再生可能とするためにシステム上必要とされるのは、第１には、通信におけるライセンス鍵を配信するための方式であり、さらに第２には、配信したいコンテンツデータを暗号化する方式そのものであり、さらに、第３には、このように配信されたコンテンツデータの無断コピーを防止するためのコンテンツデータ保護を実現する構成である。

【００５７】本発明の実施の形態においては、特に、配信、および再生の各セッションの発生時において、これらのコンテンツデータの移動先に対する認証およびチェック機能を充実させ、非認証もしくは復号鍵の破られた記録装置およびデータ再生端末（コンテンツを再生できるデータ再生端末を携帯電話機とも言う。以下同じ）に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成を説明する。

【００５８】なお、以下の説明においては、配信サーバ１０から各携帯電話機を介してメモリカードへ、またはパーソナルコンピュータからカードライタを介してメモリカードへコンテンツデータ（暗号化コンテンツデータおよびライセンス）を伝送する処理を「配信」と称することとする。

【００５９】図２は、図１に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。

【００６０】まず、配信サーバ１０より配信されるデータについて説明する。Ｄｃは、音楽データ等のコンテンツデータである。コンテンツデータＤｃは、ライセンス鍵Ｋｃで復号可能な暗号化が施される。コンテンツデータＤｃは、試聴領域Ｄｃ１と本体領域Ｄｃ２とから成り、それぞれ、異なる暗号鍵によって暗号化されている。試聴領域Ｄｃ１は、ライセンス鍵Ｋｃ１によって復号可能な暗号化が施された試聴領域｛Ｄｃ１｝Ｋｃ１と

して、また、本体領域Ｄｃ２は、ライセンス鍵Ｋｃ２によって復号可能な暗号化が施された本体領域｛Ｄｃ２｝Ｋｃ２として１つの暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを構成する。コンテンツデータＤｃは、必ず、暗号化された暗号化コンテンツデータ｛Ｄｃ｝Ｋｃとして携帯電話機１００またはパーソナルコンピュータ５０へ配信される。その結果、全体としては、コンテンツデータＤｃは、ライセンス鍵Ｋｃ（Ｋｃ１とＫｃ２とから成る）によって復号可能な暗号化が施された暗号化コンテンツデータ｛Ｄｃ｝Ｋｃとして配信サーバ１０より携帯電話機１００またはパーソナルコンピュータ５０のユーザに配布される。

【００６１】なお、以下においては、｛Ｙ｝Ｘという表記は、データＹを、復号鍵Ｘにより復号可能な暗号化を施したことを示すものとする。

【００６２】図３を参照して、情報データベース３０４が保持する暗号化コンテンツデータ｛Ｄｃ｝Ｋｃのフォーマットについて説明する。暗号化コンテンツデータ｛Ｄｃ｝Ｋｃが暗号化音楽データであるとき、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃは図３の（ａ）に示すフォーマットから成る。暗号化音楽データ９０は、試聴領域９１（｛Ｄｃ１｝Ｋｃ１）と本体領域９２（｛Ｄｃ２｝Ｋｃ２）とから成る。試聴領域９１（｛Ｄｃ１｝Ｋｃ１）は、ライセンス鍵Ｋｃ１によって復号可能である。本体領域９２（｛Ｄｃ２｝Ｋｃ２）は、ライセンス鍵Ｋｃ２によって復号可能である。試聴領域９１（｛Ｄｃ１｝Ｋｃ１）は、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃの途中に含まれ、本体領域９２（｛Ｄｃ２｝Ｋｃ２）が２分割されている。この場合、試聴用の暗号化音楽データ９１は、曲のサビから成る。試聴領域９１（｛Ｄｃ１｝Ｋｃ１）は、１つの連続する領域として示したが、本体領域９２（｛Ｄｃ２｝Ｋｃ２）と同様に、本体領域９２（｛Ｄｃ２｝Ｋｃ２）によって分割された領域であってもよい。

【００６３】また、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃは、図３の（ｂ）に示すフォーマットから成っていてもよい。暗号化音楽データ９３は、試聴用の暗号化音楽データ９４と本体用の暗号化音楽データ９５とから成る。試聴用の暗号化音楽データ９４は、ライセンス鍵Ｋｃ１によって復号可能である。本体用の暗号化音楽データ９５は、ライセンス鍵Ｋｃ２によって復号可能である。試聴用の暗号化音楽データ９４は、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃの最初に含まれている。この場合、試聴用の暗号化音楽データ９４は、曲のイントロから成る。

【００６４】図４を参照して、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃ８４の生成について説明する。平文のコンテンツデータである源データＤｃ８１を最小暗号化単位であるＭバイトの固定長を有するブロックＢＬＫ１，ＢＬＫ２，・・・，ＢＬＫｋに分割してブロックデータ８２を生成する（ｋは自然数）。最終ブロックＢＬＫｋがＭバイトに満たないときは、意味を持たないダミーデータをデータ末尾に追加してＭバイトのブロックを構成する（斜線部）。そして、ブロックＢＬＫ１，ＢＬＫ２，・・・，ＢＬＫｋの各々を個々に暗号化して暗号化データ８３を生成する。このとき、ブロックごとにライセンス鍵Ｋｃ１，Ｋｃ２のいずれに対応させるかが決定される。ライセンス鍵とブロックとの対応は付加情報Ｄｃ－ｉｎｆ内にライセンス鍵対応情報として記録される。その後、ブロックＢＬＫ１，ＢＬＫ２，・・・，ＢＬＫｋの各々にヘッダを追加して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃ８４を生成する。すなわち、ブロックＢＬＫ１は、ヘッダ８４１と、暗号化データ８４２とから成り、ブロックＢＬＫ２は、ヘッダ８４３と暗号化データ８４４とから成り、ブロックＢＬＫｋは、ヘッダ８４５と暗号化データ８４６とから成る。ヘッダ８４１，８４３，８４５は、Ｎバイトのデータであり、そのブロックが暗号化ブロックであるか非暗号化ブロックであるかを示すスクランブルフラグが記録されている。つまり、ヘッダ８４１，８４３，８４５は、暗号化ブロックであることを示す「１」または非暗号化ブロックであることを示す「０」を含む。したがって、図３の示す暗号化コンテンツデータは、図４に示すデータフォーマットから成り、試聴領域および本体領域は重複しない複数のブロックによって構成される。

【００６５】再び、図２を参照して、配信サーバ１０からは、暗号化コンテンツデータとともに、暗号化コンテンツデータに対するライセンス鍵対応情報、コンテンツデータの著作権に関する情報あるいはサーバアクセス関連情報等の平文情報としての付加情報Ｄｃ－ｉｎｆが配布される。また、ライセンスとして、ライセンス鍵Ｋｃ、配信サーバ１０からのライセンス鍵等を特定するための管理コードであるライセンスＩＤが配信サーバ１０と、携帯電話機１００またはパーソナルコンピュータ５０との間でやり取りされ、かつ、メモリカード１１０にライセンス鍵Ｋｃｉとともに記録される。さらに、ライセンスとしては、コンテンツデータＤｃを識別するためのコードであるコンテンツＩＤや、利用者側からの指定によって決定されるライセンスの種類や機能限定等の情報を含んだライセンス購入条件ＡＣに基づいて生成される、記録装置（メモリカード）におけるライセンスのアクセスに対する制限に関する情報であるアクセス制御情報ＡＣｍおよびデータ再生端末における再生に関する制御情報である再生制御情報ＡＣｐ等が存在する。具体的には、アクセス制御情報ＡＣｍはメモリカードからのライセンスまたはライセンス鍵を外部に出力するに当っての制御情報であり、再生可能回数（再生のためにライセンス鍵を出力する数）、およびライセンスの移動・複製に関する制限情報などがある。再生制御情報ＡＣｐは、再生するためにコンテンツ再生回路がライセンス鍵を受

取った後に、再生を制限する情報であり、再生期限、再生速度変更制限、再生範囲指定（部分ライセンス）などがある。

【００６６】以後、コンテンツＩＤとライセンス鍵Ｋｃｉ（ｉ＝１，２）とライセンスＩＤとアクセス制御情報ＡＣｍと再生制御情報ＡＣｐとを併せて、ライセンスと総称することとする。ライセンス鍵Ｋｃ１を含むライセンスが試聴用ライセンスであり、ライセンス鍵Ｋｃ２を含むライセンスが本体用ライセンスである。

【００６７】また、以降では、簡単化のためアクセス制御情報ＡＣｍは再生回数の制限を行なう制御情報である再生回数（０：再生不可、１～２５４：再生可能回数、２５５：制限無し）、ライセンスの移動および複製を制限する移動・複製フラグ（１：移動複製不可、２：移動のみ可、３：移動複製禁止）の２項目とし、再生制御情報ＡＣｐは再生可能な期限を規定する制御情報である再生期限（ＵＴＣｔｉｍｅコード）のみを制限するものとする。

【００６８】図５は、図１に示すデータ配信システムにおいて使用される認証のためのデータ、情報等の特性を説明する図である。

【００６９】コンテンツ再生回路、およびメモリカードには固有の公開暗号鍵ＫＰｐｙおよびＫＰｍｗがそれぞれ設けられ、公開暗号鍵ＫＰｐｙおよびＫＰｍｗはコンテンツ再生回路に固有の秘密復号鍵Ｋｐｙおよびメモリカードに固有の秘密復号鍵Ｋｍｗによってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、コンテンツ再生回路、およびメモリカードの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称し、これらの公開暗号鍵をクラス公開暗号鍵、秘密復号鍵をクラス秘密復号鍵、クラス鍵を共有する単位をクラスと称する。クラスは、製造会社や製品の種類、製造時のロット等によって異なる。

【００７０】また、コンテンツ再生回路（携帯電話機、再生端末）のクラス証明書としてＣｐｙが設けられ、メモリカードのクラス証明書としてＣｍｗが設けられる。これらのクラス証明書は、コンテンツ再生回路、およびメモリカードのクラスごとに異なる情報を有する。耐タンパモジュールが破られたり、クラス鍵による暗号が破られた、すなわち、秘密復号鍵が漏洩したクラスに対しては、禁止クラスリストにリストアップされてライセンス取得の禁止対象となる。

【００７１】これらのコンテンツ再生回路のクラス公開暗号鍵およびクラス証明書は、認証データ｛ＫＰｐｙ／／Ｃｐｙ｝ＫＰａの形式で、メモリカードのクラス公開暗号鍵およびクラス証明書は認証データ｛ＫＰｍｗ／／Ｃｍｗ｝ＫＰａの形式で、出荷時にデータ再生回路、およびメモリカードにそれぞれ記録される。後ほど詳細に説明するが、ＫＰａは配信システム全体で共通の公開認証鍵である。

【００７２】また、メモリカード１１０内のデータ処理を管理するための鍵として、メモリカードという媒体ごとに設定される公開暗号鍵ＫＰｍｃｘと、公開暗号鍵ＫＰｍｃｘで暗号化されたデータを復号することが可能なそれぞれに固有の秘密復号鍵Ｋｍｃｘが存在する。このメモリカードごとに個別な公開暗号鍵および秘密復号鍵を総称して個別鍵と称し、公開暗号鍵ＫＰｍｃｘを個別公開暗号鍵、秘密復号鍵Ｋｍｃｘを個別秘密復号鍵と称する。

【００７３】メモリカード外とメモリカード間でのデータ授受でのデータ授受における秘密保持のための暗号鍵として、コンテンツデータの配信、および再生が行なわれるごとに配信サーバ１０、携帯電話機１００、およびメモリカード１１０において生成される共通鍵Ｋｓ１～Ｋｓ３が用いられる。

【００７４】ここで、共通鍵Ｋｓ１～Ｋｓ３は、配信サーバ、コンテンツ再生回路もしくはメモリカード間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵Ｋｓ１～Ｋｓ３を「セッションキー」とも呼ぶこととする。

【００７５】これらのセッションキーＫｓ１～Ｋｓ３は、各セッションごとに固有の値を有することにより、配信サーバ、コンテンツ再生回路、およびメモリカードによって管理される。具体的には、セッションキーＫｓ１は、配信サーバによって配信セッションごとに発生される。セッションキーＫｓ２は、メモリカードによって配信セッションおよび再生セッションごとに発生し、セッションキーＫｓ３は、コンテンツ再生回路において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行した上でライセンス鍵等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【００７６】なお、カードライタ８０とＵＳＢケーブル７０を介してパーソナルコンピュータ５０とメモリカード１１０との間の通信においては、配信サーバ１０と携帯電話機１００の機能をパーソナルコンピュータ５０に読替え、メモリカードインタフェース１２００をカードライタ８０およびＵＳＢケーブル７０に読替えればよい。

【００７７】図６は、図１に示した配信サーバ１０の構成を示す概略ブロック図である。配信サーバ１０は、コンテンツデータを所定の方式に従って暗号化したデータやコンテンツＩＤ等の配信情報を保持するための情報データベース３０４と、携帯電話機の各ユーザごとにコンテンツデータへのアクセス開始に従った課金情報を保持するための課金データベース３０２と、情報データベース３０４に保持されたコンテンツデータのメニューを保

17

持するメニューデータベース３０７と、ライセンスの配信ごとにコンテンツデータおよびライセンス鍵等の配信を特定するトランザクションＩＤ等の配信に関するログを保持する配信記録データベース３０８と、情報データベース３０４、課金データベース３０２、メニューデータベース３０７、および配信記録データベース３０８からのデータをバスＢＳ１を介して受取り、所定の処理を行なうためのデータ処理部３１０と、通信網を介して、配信キャリア２０とデータ処理部３１０との間でデータ授受を行なうための通信装置３５０とを備える。

【００７８】暗号化コンテンツデータ｛Ｄｃ｝Ｋｃが朗読データ、教材データ、またはゲームソフトのデータであるとき、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃは、図１３の（ｃ）に示すフォーマットから成る。暗号化コンテンツデータ９６は、複数の領域９６１～９６７から成る。各領域９６１～９６７は、それぞれ、ライセンス鍵Ｋｃ１，Ｋｃ２，Ｋｃ３，Ｋｃ４，Ｋｃ５，Ｋｃ６，Ｋｃ７によって復号可能である。

【００７９】暗号化コンテンツデータ｛Ｄｃ｝Ｋｃが既に説明した音楽データと同様に試しようの領域を備えたビデオデータであるとき、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃは、図１３の（ｄ）に示すフォーマットから成る。暗号化データ９７は、付属用の領域９７１と本体用の領域９７２とから成る。付属用の領域９７１は、ライセンス鍵Ｋｃ１によって復号可能である。本体用の領域９７２は、ライセンス鍵Ｋｃ２によって復号可能である。付属用の領域９７１は、ビデオまたはゲームのサブタイトルから成る。暗号化コンテンツデータ９６，９７の復号については、図７に示すコンテンツ再生回路１５５０が受理可能である。この場合、音楽再生部１５２０が各コンテンツに適合した再生回路に置換えられる。

【００８０】データ処理部３１０は、バスＢＳ１上のデータに応じて、データ処理部３１０の動作を制御するための配信制御部３１５と、配信制御部３１５に制御されて、配信セッション時にセッションキーＫｓ１を発生するためのセッションキー発生部３１６と、メモリカードから送られてきた認証のための認証データ｛ＫＰｍｗ／／Ｃｍｗ｝ＫＰａを復号するための２種類の公開認証鍵ＫＰａを保持する認証鍵保持部３１３と、メモリカードから送られてきた認証のための認証データ｛ＫＰｍｗ／／Ｃｍｗ｝ＫＰａを通信装置３５０およびバスＢＳ１を介して受けて、認証鍵保持部３１３からの公開認証鍵ＫＰａによって復号処理を行なう復号処理部３１２と、配信セッションごとに、セッション鍵Ｋｓ１を発生するセッションキー発生部３１６、セッションキー発生部３１６より生成されたセッションキーＫｓ１を復号処理部３１２によって得られたクラス公開暗号鍵ＫＰｍｗを用いて暗号化して、バスＢＳ１に出力するための暗号化処理部３１８と、セッションキーＫｓ１によって暗号化された上で送信されたデータをバスＢＳ１より受けて、復号処理を行なう復号処理部３２０とを含む。

18

【００８１】データ処理部３１０は、さらに、配信制御部３１５から与えられるライセンス鍵Ｋｃおよびアクセス制御情報ＡＣｍを、復号処理部３２０によって得られたメモリカードごとに個別公開暗号鍵ＫＰｍｃｘによって暗号化するための暗号化処理部３２６と、暗号化処理部３２６の出力を、復号処理部３２０から与えられるセッションキーＫｓ２によってさらに暗号化してバスＢＳ１に出力するための暗号化処理部３２８とを含む。

【００８２】配信サーバ１０の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【００８３】図７は、図１に示した携帯電話機１００の構成を説明するための概略ブロック図である。

【００８４】携帯電話機１００は、携帯電話機１００の各部のデータ授受を行なうためのバスＢＳ２と、携帯電話網により無線伝送される信号を受信するためのアンテナ１１０１と、アンテナからの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナ１１０１に与えるための送受信部１１０２とを含む。

【００８５】携帯電話機１００は、さらに、携帯電話機１００のユーザの音声データを取込むためのマイク１１０３と、マイク１１０３からの音声データをアナログ信号からディジタル信号に変換するＡＤ変換器１１０４と、ＡＤ変換器１１０４からの音声データを所定の方式に変調する音声符号化部１１０５とを含む。

【００８６】携帯電話器１００は、さらに、アンテナ１１０１および送受信部１１０２を介して受信した他の携帯電話機のユーザの音声データを再生する音声再生部１１０６と、音声再生部１１０６からのデータをディジタル信号からアナログ信号へ変換するＤＡ変換器１１０７と、ＤＡ変換器１１０７からの音声データを外部へ出力するスピーカ１１０８とを含む。

【００８７】携帯電話機１００は、さらに、バスＢＳ２を介して携帯電話機１００の動作を制御するためのコントローラ１１０９と、外部からの指示を携帯電話機１００に与えるための操作パネル１１１１と、コントローラ１１０９等から出力される情報をユーザに視覚情報として与えるための表示パネル１１１０とを含む。

【００８８】携帯電話機１００は、さらに、配信サーバ１０からのコンテンツデータ（音楽データ）を記憶し、かつ、復号処理を行なうための着脱可能なメモリカード１１０と、メモリカード１１０とバスＢＳ２との間のデータの授受を制御するためのメモリカードインタフェース１２００とを含む。

【００８９】携帯電話機１００は、さらに、クラス公開暗号鍵ＫＰｐ１およびクラス証明書Ｃｐ１を公開認証鍵ＫＰａで復号することでその正当性を認証できる状態に暗号化した認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを

19

保持する認証データ保持部１５００を含む。ここで、再生端末１０２のクラスｙは、ｙ＝１であるとする。

【００９０】携帯電話機１００は、さらに、クラス固有の復号鍵であるＫｐ１を保持するＫｐ１保持部１５０２と、バスＢＳ２から受けたデータをＫｐ１によって復号し、メモリカード１１０によって発生されたセッションキーＫｓ２を得る復号処理部１５０４とを含む。

【００９１】携帯電話機１００は、さらに、メモリカード１１０に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード１１０との間でバスＢＳ２上においてやり取りされるデータを暗号化するためのセッションキーＫｓ３を乱数等により発生するセッションキー発生部１５０８と、暗号化コンテンツデータの再生セッションにおいてメモリカード１１０からライセンス鍵Ｋｃ（Ｋｃ１とＫｃ２とから成る。以下同じ）および再生制御情報ＡＣｐを受取る際に、セッションキー発生部１５０８により発生されたセッションキーＫｓ３を復号処理部１５０４によって得られたセッションキーＫｓ２によって暗号化し、バスＢＳ２に出力する暗号化処理部１５０６とを含む。

【００９２】携帯電話機１００は、さらに、バスＢＳ２上のデータをセッションキーＫｓ３によって復号して、ライセンス鍵Ｋｃおよび再生制御情報ＡＣｐを出力する復号処理部１５１０と、コントローラ１１０９からの指示によって復号処理部１５１０から出力されたライセンス鍵Ｋｃ１，Ｋｃ２のいずれか一方を端子１５１２を介してＫｃ保持部１５１４へ出力し、端子１５１３を介してライセンス鍵Ｋｃ１，Ｋｃ２のいずれか他方をＫｃ保持部１５１５へ出力するスイッチ１５１１とを含む。

【００９３】携帯電話機１００は、さらに、端子１５１２から入力されたライセンス鍵Ｋｃ１，Ｋｃ２のいずれかを保持するＫｃ保持部１５１４と、端子１５１３から入力されたＫｃ保持部１５１４が保持するライセンス鍵とは異なるライセンス鍵、すなわち、Ｋｃ保持部１５１４がライセンス鍵Ｋｃ１を保持するときライセンス鍵Ｋｃ２を保持するＫｃ保持部１５１５とを含む。

【００９４】携帯電話機１００は、さらに、Ｋｃ保持部１５１４またはＫｃ保持部１５１５に保持される２つのライセンス鍵Ｋｃ１，Ｋｃ２のいずれか１つを選択して復号処理部１５１９へ出力するスイッチ１５１８を含む。スイッチ１５１８は、Ｋｃ保持部１５１４からのライセンス鍵を受ける端子１５１６と、Ｋｃ保持部１５１５からのライセンス鍵を受ける端子１５１７とを含む。なお、スイッチ１５１８は、コントローラ１１０９からの指示によって端子１５１６または端子１５１７を選択してライセンス鍵Ｋｃ１またはライセンス鍵Ｋｃ２を復号処理部１５１９へ出力する。

【００９５】携帯電話機１００は、さらに、バスＢＳ２より暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを受けて、スイッチ１５１８から入力されたライセンス鍵Ｋｃ１またはＫｃ２によって暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを復号する復号処理部１５１９とを含む。試聴用ライセンスのみをメモリカード１１０に記録している場合には、ライセンス鍵Ｋｃ１にて復号再生可能な試聴領域｛Ｄｃ１｝Ｋｃ１のみ再生可能である。

20

【００９６】携帯電話機１００は、さらに、復号処理部１５１９からの出力を受けてコンテンツデータを再生するための音楽再生部１５２０と、音楽再生部１５２０の出力をディジタル信号からアナログ信号に変換するＤＡ変換器１５２１と、ＤＡ変換器１５２１の出力をヘッドホーンなどの外部出力装置（図示省略）へ出力するための端子１５２２とを含む。

【００９７】なお、図７においては、点線で囲んだ領域は暗号化コンテンツデータを復号して音楽データを再生するコンテンツ再生回路１５５０を構成する。

【００９８】携帯電話機１００の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【００９９】図８は、図１に示すメモリカード１１０の構成を説明するための概略ブロック図である。

【０１００】既に説明したように、メモリカードのクラス公開暗号鍵およびクラス秘密復号鍵として、ＫＰｍｗおよびＫｍｗが設けられ、メモリカードのクラス証明書Ｃｍｗが設けられるが、メモリカード１１０においては、自然数ｗ＝３で表わされるものとする。また、メモリカードを識別する自然数ｘはｘ＝４で表されるものとする。

【０１０１】したがって、メモリカード１１０は、認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを保持する認証データ保持部１４００と、メモリカードごとに設定される固有の復号鍵である個別秘密復号鍵Ｋｍｃ４を保持するＫｍｃ保持部1402と、クラス秘密復号鍵Ｋｍ３を保持するＫｍ保持部１４２１と、個別秘密復号鍵Ｋｍｃ４によって復号可能な公開暗号鍵ＫＰｍｃ４を保持するＫＰｍｃ保持部１４１６とを含む。

【０１０２】このように、メモリカードという記録装置の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたライセンス鍵の管理をメモリカード単位で実行することが可能になる。

【０１０３】メモリカード１１０は、さらに、メモリカードインタフェース１２００との間で信号を端子１４２６を介して授受するインタフェース１４２４と、インタフェース１４２４との間で信号をやり取りするバスＢＳ４と、バスＢＳ４にインタフェース１４２４から与えられるデータから、クラス秘密復号鍵Ｋｍ３をＫｍ保持部１４２１から受けて、配信サーバ１０が配信セッションにおいて生成したセッションキーＫｓ1を接点Ｐａに出力する復号処理部１４２２と、ＫＰａ保持部１４１４から公開認証鍵ＫＰａを受けて、バスＢＳ４に与えられる

データから公開認証鍵ＫＰａによる復号処理を実行して復号結果と得られたクラス証明書をコントローラ１４２０に、得られたクラス公開鍵を暗号化処理部１４１０に出力する復号処理部１４０８と、切換スイッチ１４４２によって選択的に与えられる鍵によって、切換スイッチ１４４６によって選択的に与えられるデータを暗号化してバスＢＳ４に出力する暗号化処理部１４０６とを含む。

【０１０４】メモリカード１１０は、さらに、配信、および再生の各セッションにおいてセッションキーＫｓ２を発生するセッションキー発生部１４１８と、セッションキー発生部１４１８の出力したセッションキーＫｓ２を復号処理部１４０８によって得られるクラス公開暗号鍵ＫＰｐｙもしくはＫＰｍｗによって暗号化してバスＢＳ４に送出する暗号化処理部１４１０と、バスＢＳ４よりセッションキーＫｓ２によって暗号化されたデータを受けてセッションキー発生部１４１８より得たセッションキーＫｓ２によって復号する復号処理部１４１２と、暗号化コンテンツデータの再生セッションにおいてメモリ１４１５から読出されたライセンス鍵Ｋｃおよび再生制御情報ＡＣｐを、復号処理部１４１２で復号された他のメモリカード１１０の個別公開暗号鍵ＫＰｍｃｘ（ｘ≠４）で暗号化する暗号処理部１４１７とを含む。

【０１０５】メモリカード１１０は、さらに、バスＢＳ４上のデータを個別公開暗号鍵ＫＰｍｃ４と対をなすメモリカード１１０の個別秘密復号鍵Ｋｍｃ４によって復号するための復号処理部１４０４と、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを再生するためのライセンス（Ｋｃ，ＡＣｐ，ＡＣｍ，ライセンスＩＤ，コンテンツＩＤ）と、付加情報Ｄｃ－ｉｎｆとをバスＢＳ４より受けて格納するためのメモリ１４１５とを含む。メモリ１４１５は、例えば半導体メモリによって構成される。また、メモリ１４１５は、ライセンス領域１４１５Ａと、データ領域１４１５Ｂとから成る。ライセンス領域１４１５Ａは、ライセンスを記録するための領域である。データ領域１４１５Ｂは、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃ、および暗号化コンテンツデータの付加情報Ｄｃ－ｉｎｆを記録するための領域である。なお、データ領域１４１５Ｂは、外部からアクセス可能である。

【０１０６】メモリカード１１０は、さらに、バスＢＳ４を介して外部との間でデータ授受を行ない、バスＢＳ４との間で再生情報等を受けて、メモリカード１１０の動作を制御するためのコントローラ１４２０を含む。

【０１０７】なお、ライセンス領域１４１５Ａは、耐タンパモジュール領域に構成される。また、ライセンス領域１４１５Ａとデータ領域１４１５Ｂとは、１つのメモリ１４１５内に構成されている必要はなく、それぞれ、別々に構成されていても良い。さらに、メモリ１４１５は、データ領域１４１５Ｂを伴わないライセンス専用の領域であってもよい。

【０１０８】以下、図１に示すデータ配信システムにおける各セッションの動作について説明する。

【０１０９】［試聴用配信］図１に示す配信サーバ１０は、携帯電話網を介して携帯電話機１００に装着されたメモリカード１１０に暗号化音楽データ｛Ｄｃ｝Ｋｃ、ライセンス鍵Ｋｃ１を含む試聴用ライセンス、およびライセンス鍵Ｋｃ２を含む本体用ライセンスを配信する動作について説明する。図９は、配信サーバ１０からメモリカード１１０への暗号化音楽データ｛Ｄｃ｝Ｋｃ、ライセンス鍵Ｋｃ１を含む試聴用ライセンス、およびライセンスＫｃ１，Ｋｃ２の配信の全体動作を示すフローチャートである。携帯電話機１００は、携帯電話機１００のユーザの指示に応じて、携帯電話網を介して配信サーバ１０へ暗号化音楽データ｛Ｄｃ｝Ｋｃおよびライセンス鍵Ｋｃ１を含む試聴用ライセンスの配信要求を送信し、配信サーバ１０から暗号化音楽データ｛Ｄｃ｝Ｋｃおよび試聴用ライセンスを受信する。そして、携帯電話機１００は、受信した暗号化音楽データ｛Ｄｃ｝Ｋｃおよびライセンス鍵Ｋｃ１を含む試聴用ライセンスをメモリカード１１０に記録する（ステップＳ１０）。その後、携帯電話機１００は、ユーザからの試聴指示に応じて、メモリカード１１０から暗号化音楽データ｛Ｄｃ｝Ｋｃの一部である試聴領域｛Ｄｃ１｝Ｋｃ１およびライセンス鍵Ｋｃ１を読出し、コンテンツ再生回路１５５０において試聴用のライセンスに含まれるライセンス鍵Ｋｃ１によって復号可能な暗号化音楽データ｛Ｄｃ１｝Ｋｃ１を復号および再生する。そして、ユーザは、再生された音楽データをヘッドホーン１３０を介して試聴する（ステップＳ２０）。

【０１１０】ユーザは、試聴した音楽データの購入を希望するとき、ライセンス鍵Ｋｃ２を含む本体用ライセンスのダウンロード要求を携帯電話機１００に入力する。そうすると、携帯電話機１００は、携帯電話網を介してライセンス鍵Ｋｃ２を含む本体用ライセンスの配信要求を配信サーバ１０へ送信し、配信サーバ１０からライセンス鍵Ｋｃ２を含む本体用ライセンスを受信し、その受信したライセンス鍵Ｋｃ２を含む本体用ライセンスをメモリカード１１０に記録する（ステップＳ３０）。その後、携帯電話機１００は、ユーザの再生要求に応じて、暗号化音楽データ｛Ｄｃ｝Ｋｃおよび２つのライセンス鍵Ｋｃ１，Ｋｃ２をメモリカード１１０から読出し、コンテンツ再生回路１５５０において暗号化音楽データ｛Ｄｃ｝Ｋｃを、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃの各領域に適合したライセンス鍵Ｋｃ１およびライセンス鍵Ｋｃ２を用いて復号および再生する。

【０１１１】以下、ステップＳ１０，Ｓ２０，Ｓ３０の詳細について説明する。図１０および図１１は、図９のステップＳ１０およびステップＳ３０におけるライセンスの配信処理の詳細な動作を説明するためのフローチャ

ートである。まず、試聴用のライセンスおよび暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを配信サーバ１０からダウンロードするステップＳ１０の詳細について説明する。

【０１１２】図１０における処理以前に、携帯電話機１００のユーザは、配信サーバ１０に対して電話網を介して接続し、購入を希望するコンテンツに対するコンテンツＩＤを取得し、必要とするライセンスの種類を決定していることを前提としている。また、フローチャートにおけるライセンス鍵Ｋｃｉ（ｉ＝１，２）は、Ｋｃ１またはＫｃ２のいずれかのライセンス鍵であり、この場合、ライセンス鍵Ｋｃ１を含む試聴用ライセンスの取得を目的としているため、ｉ＝１である。図１０および図１１におけるライセンス鍵Ｋｃｉのｉをｉ＝１と読替えて試聴用ライセンスの配信を説明する。

【０１１３】図１０を参照して、携帯電話機１００のユーザから操作パネル１１１１を介してコンテンツＩＤの指定による配信リクエストがなされる（ステップＳ１００）。そして、操作パネル１１１１を介して試聴用の暗号化音楽データ｛Ｄｃ１｝Ｋｃ１のライセンスＫｃ１を購入するための購入条件ＡＣが入力される（ステップＳ１０２）。つまり、選択した暗号化音楽データ｛Ｄｃ｝Ｋｃを復号するライセンス鍵Ｋｃｉをダウンロードするための条件として、ライセンス鍵Ｋｃ１なのか、ライセンス鍵Ｋｃ２なのか、すなわち試聴用ライセンスなのか本体用ライセンスなのかを指示する。さらに、本体用ライセンスの場合には、暗号化コンテンツデータのアクセス制御情報ＡＣｍ、および再生制御情報ＡＣｐを設定するための条件がライセンス購入条件ＡＣとして入力される。

【０１１４】暗号化コンテンツデータの購入条件ＡＣが入力されると、コントローラ１１０９は、バスＢＳ２およびメモリカードインタフェース１２００を介してメモリカード１１０へ認証データの出力指示を与える（ステップＳ１０４）。メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ４を介して認証データの送信要求を受信する（ステップＳ１０６）。そして、コントローラ１４２０は、バスＢＳ４を介して認証データ保持部１４００から認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを読出し、｛ＫＰｍ３／／Ｃｍ３｝ＫＰａをバスＢＳ４、インタフェース１４２４および端子１４２６を介して出力する（ステップＳ１０８）。

【０１１５】携帯電話機１００のコントローラ１１０９は、メモリカード１１０からの認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａに加えて、コンテンツＩＤ、ライセンス購入条件のデータＡＣ、および配信リクエストを配信サーバ１０に対して送信する（ステップＳ１１０）。

【０１１６】配信サーバ１０では、携帯電話機１００から配信リクエスト、コンテンツＩＤ、認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ、およびライセンス購入条件のデータＡＣを受信し（ステップＳ１１２）、復号処理部３１２においてメモリカード１１０から出力された認証データを公開認証鍵ＫＰａで復号処理を実行する（ステップＳ１１４）。

【０１１７】配信制御部３１５は、復号処理部３１２における復号処理結果から、正規の機関でその正当性を証明するための暗号化を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ１１６）。正当な認証データであると判断された場合、配信制御部３１５は、クラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を承認し、受理する。そして、次の処理（ステップＳ１１８）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を受理しないで配信セッションを終了する（ステップＳ１６４）。

【０１１８】認証の結果、正当な認証データを持つメモリカードを装着した携帯電話機からのアクセスであることが確認されると、配信サーバ１０において、セッションキー発生部３１６は、配信のためのセッションキーＫｓ１を生成する（ステップＳ１１８）。セッションキーＫｓ１は、復号処理部３１２によって得られたメモリカード１１０に対応するクラス公開暗号鍵ＫＰｍ３によって、暗号化処理部３１８によって暗号化される（ステップＳ１２０）。

【０１１９】配信制御部３１５は、ライセンスＩＤを生成し（ステップＳ１２２）、ライセンスＩＤおよび暗号化されたセッションキーＫｓ１は、ライセンスＩＤ／／｛Ｋｓ１｝Ｋｍ３として、バスＢＳ１および通信装置３５０を介して外部に出力される（ステップＳ１２４）。

【０１２０】携帯電話機１００が、ライセンスＩＤ／／｛Ｋｓ１｝Ｋｍ３を受信すると、コントローラ１１０９は、ライセンスＩＤ／／｛Ｋｓ１｝Ｋｍ３をメモリカード１１０に入力する（ステップＳ１２６）。そうすると、メモリカード１１０においては、端子１４２６およびインタフェース１４２４を介して、コントローラ１４２０は、ライセンスＩＤ／／｛Ｋｓ１｝Ｋｍ３を受理する（ステップＳ１２８）。そして、コントローラ１４２０は、バスＢＳ４を介して｛Ｋｓ１｝Ｋｍ３を復号処理部１４２２へ与え、復号処理部１４２２は、保持部１４２１に保持されるメモリカード１１０に固有なクラス秘密復号鍵Ｋｍ３によって復号処理することにより、セッションキーＫｓ１を復号し、セッションキーＫｓ１を受理する（ステップＳ１３２）。

【０１２１】コントローラ１４２０は、配信サーバ１０で生成されたセッションキーＫｓ１の受理を確認すると、セッションキー発生部１４１８に対してメモリカード１１０において配信動作時に生成されるセッションキーＫｓ２の生成を指示する。そして、セッションキー発生部１４１８は、セッションキーＫｓ２を生成する（ステップＳ１３４）。

【０１２２】暗号化処理部１４０６は、切換スイッチ１４４２の接点Ｐａを介して復号処理部１４２２より与えられるセッションキーＫｓ１によって、切換スイッチ１４４６の接点を順次切換えることによって与えられるセッションキーＫｓ２、および個別公開暗号鍵ＫＰｍｃ４を１つのデータ列として暗号化して、｛Ｋｓ２／／ＫＰｍｃ４｝Ｋｓ１をバスＢＳ４に出力する。バスＢＳ４に出力された暗号化データ｛Ｋｓ２／／ＫＰｍｃ４｝Ｋｓ１は、バスＢＳ４からインタフェース１４２４および端子１４２６を介して携帯電話機１００に出力され（ステップＳ１３８）、携帯電話機１００から配信サーバ１０に送信される（ステップＳ１４０）。

【０１２３】図１１を参照して、配信サーバ１０は、｛Ｋｓ２／／ＫＰｍｃ４｝Ｋｓ１を受信して、復号処理部３２０においてセッションキーＫｓ１による復号処理を実行し、メモリカード１１０で生成されたセッションキーＫｓ２、およびメモリカード１１０に固有の公開暗号鍵ＫＰｍｃ４を受理する（ステップＳ１４２）。

【０１２４】配信制御部３１５は、ステップＳ１１２で取得したコンテンツＩＤと購入条件ＡＣに従ってライセンス鍵Ｋｃ１を情報データベース３０４から取得し（ステップＳ１４４）、ステップＳ１１２で取得したライセンス購入条件のデータＡＣに従って、アクセス制御情報ＡＣｍおよび再生制御情報ＡＣｐを決定する（ステップＳ１４６）。

【０１２５】配信制御部３１５は、生成したライセンス、すなわち、ライセンスＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、再生制御情報ＡＣｐ、およびアクセス制御情報ＡＣｍを暗号化処理部３２６に与える。暗号化処理部３２６は、復号処理部３２０によって得られたメモリカード１１０に固有の公開暗号鍵ＫＰｍｃ４によってライセンスを暗号化して暗号化データ｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ１／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４を生成する（ステップＳ１４８）。そして、暗号化処理部３２８は、暗号化処理部３２６からの暗号化データ｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ１／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４を、復号処理部３２０からのセッションキーＫｓ２によって暗号化し、暗号化データ｛｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ１／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を出力する。配信制御部３１５は、バスＢＳ１および通信装置３５０を介して暗号化データ｛｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ１／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を携帯電話機１００へ送信する（ステップＳ１５０）。

【０１２６】携帯電話機１００は、送信された暗号化データ｛｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ１／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を受信し、バスＢＳ２を介してメモリカード１１０に入力する（ステップＳ１５２）。メモリカード１１０においては、端子１４２６およびインタフェース１４２４を介して、バスＢＳ４に与えられた受信データを復号処理部１４１２によって復号する。復号処理部１４１２は、セッションキー発生部１４１８から与えられたセッションキーＫｓ２を用いてバスＢＳ４の受信データを復号し、バスＢＳ４に出力する（ステップＳ１５４）。

【０１２７】この段階で、バスＢＳ４には、Ｋｍｃ保持部１４０２に保持される秘密復号鍵Ｋｍｃ４で復号可能な暗号化ライセンス｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ１／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝が出力される（ステップＳ１５４）。

【０１２８】コントローラ１４２０の指示によって、暗号化ライセンス｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ１／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４は、復号処理部１４０４において、個別秘密復号鍵Ｋｍｃ４によって復号され、ライセンス（ライセンス鍵Ｋｃ１、ライセンスＩＤ、コンテンツＩＤ、アクセス制御情報ＡＣｍおよび再生制御情報ＡＣｐ）が受理される（ステップＳ１５６）。

【０１２９】そうすると、メモリカード１１０のコントローラ１４２０は、受理したライセンス（ライセンスＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ１、アクセス制御情報ＡＣｍ、および再生制御情報ＡＣｐ）を、ライセンス領域１４１５Ａに格納する（ステップＳ１６０）。そして、配信サーバ１０において、課金処理が行なわれる。すなわち、配信制御部３１５は、課金情報を課金データベース３０２に記録する（ステップＳ１６２）。なお、この場合の試聴用ライセンスの配信に対する課金料金は、後述する本体用ライセンスの配信に対する課金料金よりも低い。そして、ライセンスの配信動作は終了する（ステップＳ１６４）。

【０１３０】暗号化コンテンツデータ｛Ｄｃ｝Ｋｃについては、単なるダウンロード処理であるため詳細には説明しないが、試聴用ライセンスの配信動作が終了した後、携帯電話機１００のコントローラ１１０９は、暗号化コンテンツデータの配信要求を配信サーバ１０へ送信し、配信サーバ１０は、暗号化コンテンツデータの配信要求を受信する。そして、配信サーバ１０の配信制御部３１５は、情報データベース３０４より、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを取得して、これらのデータをバスＢＳ１および通信装置３５０を介して出力する。

【０１３１】携帯電話機１００は、｛Ｄｃ｝Ｋｃ／／Ｄｃ－ｉｎｆを受信して、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを受理する。そうすると、コントローラ１１０６は、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆをバスＢＳ２およびメモリカードインタフェース１２００を介してメモリカード１１０に入力する。メモリカード１１０のコントローラ１４２０は、受理した暗号化コンテンツ

データ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆをメモリ１４１５のデータ領域１４１５Ｂに記録する。なお、付加情報Ｄｃ－ｉｎｆには、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃのうち、どのブロックをどのライセンス鍵によって復号すべきかを示すライセンス鍵を変更するためのライセンスとブロックの対応情報とが含まれる。

【０１３２】このようにして、ライセンスの配信においては、携帯電話機１００に装着されたメモリカード１１０が正規の認証データを保持する機器であること、同時に、クラス証明書Ｃｍ３とともに暗号化して送信できた公開暗号鍵ＫＰｍ３が有効であることを確認した上でコンテンツデータを配信することができ、不正なメモリカードへのコンテンツデータの配信を禁止することができる。

【０１３３】さらに、配信サーバおよびメモリカードでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。

【０１３４】なお、上記において、試聴用ライセンスの配信に対して課金するとして説明したが（ステップＳ１６２）、試聴は、本体用ライセンスをダウンロードしてもらうことを目的としたサービスであり、より多くのユーザに聴いてもらう必要があるため、試聴用ライセンスの配信に対しては課金をしないことも可能である。

【０１３５】［試聴］次に、ステップＳ２０における試聴について詳細に説明する。試聴用の再生においては、携帯電話機１００のコントローラ１１０９は、メモカード１１０から再生を行なう楽曲の付加データＤｃ－ｉｎｆを読出して、試聴用ライセンスにて再生可能な試聴用領域｛Ｄｃ１｝Ｋｃ１を構成するブロックを特定し、特定されたブロックのみにて構成される１つの新しい暗号化コンテンツデータを仮想的に生成し、この仮想的に生成された暗号化コンテンツデータを復号して再生する。図３の（ａ）を参照して、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃが暗号化コンテンツデータ９０である場合には、試聴領域９１（｛Ｄｃ１｝Ｋｃ１）を構成するブロックを確認し、該当するブロックのみから構成されるデータ列を一つの楽曲として再生する。　図３の（ｂ）を参照して、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃが暗号化コンテンツデータ９３である場合も同様に、試聴領域９４（｛Ｄｃ１｝Ｋｃ１）を一つの楽曲として再生する。

【０１３６】再生は、まず、メモリカード１１０に格納されている試聴用ライセンスに含まれるライセンス鍵Ｋｃ１をコンテンツ再生回路１５５０内の２つのＫｃ保持部１５１４，１５１５のいずれかに保持させる「再生許諾」と、「再生許諾」後に、Ｋｃ保持部１５１４，１５１５のいずれかに保持されているライセンス鍵Ｋｃ１をスイッチ１５１８にて選択して復号処理部１５１９に供給する。試聴用に仮想的に構成された暗号化コンテンツデータは試聴用領域｛Ｄｃ１｝Ｋｃ１と対応する。したがって、試聴用に仮想的に構成された暗号化コンテンツデータを、暗号化コンテンツデータ｛Ｄｃ１｝Ｋｃ１とも表すものとする。

【０１３７】そうすると、コントローラ１１０９はメモリカード１１０から暗号化コンテンツデータ｛Ｄｃ１｝Ｋｃ１を構成するブロックを再生順序に従って読出して復号処理部１５１９に供給する。復号処理部１５１９は、入力された暗号化コンテンツデータを構成するブロックをライセンス鍵Ｋｃ１によって、それぞれ復号し、暗号化コンテンツデータ｛Ｄｃ１｝Ｋｃ１を復号して得られるコンテンツデータを構成する平文化されたブロック（源データを構成するブロック）を抽出する。そして、復号処理部１５１９は、抽出したブロックを音楽再生部１５２０に出力する。音楽再生部１５２０は、復号処理部１５１９から供給されるブロックに含まれるデータに基づいて、音楽をデジタル再生し、ＡＤ変換器１５２１へ供給する。そうすると、ＡＤ変換器１５２１は、コンテンツデータをデジタル信号からアナログ信号に変換して端子１５２２へ出力する。そして、暗号化コンテンツデータ｛Ｄｃ１｝Ｋｃ１を構成する全てのブロックが再生順に、メモリカード１１０から読出され、一連の処理が終了すると試聴用の再生が終了する。ユーザは、端子１５２２に接続されたヘッドホーン１３０等によってこの暗号化コンテンツデータ｛Ｄｃ｝Ｋｃの試聴領域｛Ｄｃ１｝Ｋｃ１を試聴することができる。

【０１３８】このとき、再生の対象となる全てのブロックに対する一連の処理が終了すると試聴用の再生が終了すると説明したが、繰り返し試聴することを前提として、再生の対象となる全てのブロックの読出しが終了すると、暗号化コンテンツデータ｛Ｄｃ１｝Ｋｃ１の先頭のブロックにもどって連続して再生するように構成することも可能である。この場合、試聴の終了は、ユーザが操作パネル１１１１を操作して、試聴の終了をコントローラ１１０９に指示し、コントローラ１１０９が、指示に従って再生を終了するように構成する。

【０１３９】次に、試聴用ライセンスに含まれるライセンス鍵Ｋｃ１をコンテンツ再生回路１５５０内の２つのＫｃ保持部１５１４，１５１５のいずれかに保持させる「再生許諾」について説明する。図１２は「再生許諾」の動作を説明するためのフローチャートである。「再生許諾」は試聴用ライセンスのライセンス鍵Ｋｃ１をＫｃ保持部１５１４，１５１５のいずれかに保持させるのみでなく、本体用ライセンスのライセンス鍵Ｋｃ２をＫｃ保持部１５１４，１５１５のいずれかに保持させる処理でもあり、図１２ではライセンス鍵はＫｃｉと表記されている。試聴においてはライセンス鍵を区別する識別子

ｉがｉ＝１と読替えて説明を行なう。また、ライセンス鍵Ｋｃ１はＫｃ保持部１５１４に保持されるものとして説明を行なう。

【０１４０】図１２を参照して、試聴のための再生動作が開始されると、携帯電話機１００のユーザから操作パネル１１１１を介して再生許諾リクエストが携帯電話機１００にインプットされる（ステップＳ２００）。そうすると、コントローラ１１０９は、バスＢＳ２を介して認証データの出力要求をコンテンツ再生回路１５５０に行ない（ステップＳ２０２）、コンテンツ再生回路１５５０は認証データの出力要求を受信する（ステップＳ２０４）。そして、認証データ保持部１５００は、認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを出力し（ステップＳ２０６）、コントローラ１１０９は、メモリカードインタフェース１２００を介してメモリカード１１０へ認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを入力する（ステップＳ２０８）。

【０１４１】そうすると、メモリカード１１０は、認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを受理し、復号処理部１４０８は、受理した認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを、ＫＰａ保持部１４１４に保持された公開認証鍵ＫＰａによって復号し（ステップＳ２１０）、コントローラ１４２０は復号処理部１４０８における復号処理結果から、認証処理を行なう。すなわち、認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａが正規の認証データであるか否かを判断する認証処理を行なう（ステップＳ２１２）。復号できなかった場合、ステップＳ２６０へ移行し、再生動作は終了する。認証データが復号できた場合、コントローラ１４２０は、セッションキー発生部１４１８を制御し、セッションキー発生部１４１８は、再生セッション用のセッションキーＫｓ２を発生させる（ステップＳ２１４）。そして、暗号処理部１４１０は、セッションキー発生部１４１８からのセッションキーＫｓ２を、復号処理部１４０８で復号された公開暗号鍵ＫＰｐ１によって暗号化した｛Ｋｓ２｝Ｋｐ１をバスＢＳ４へ出力する。そうすると、コントローラ１４２０は、インタフェース１４２４および端子１４２６を介してメモリカードインタフェース１２００へ｛Ｋｓ２｝Ｋｐ１を出力する（ステップＳ２１６）。携帯電話機１００のコントローラ１１０９は、メモリカードインタフェース１２００を介して｛Ｋｓ２｝Ｋｐ１を取得する。そして、コントローラ１１０９は、｛Ｋｓ２｝Ｋｐ１をバスＢＳ２を介してコンテンツ再生回路１５５０の復号処理部１５０４へ与え（ステップＳ２１８）、復号処理部１５０４は、Ｋｐ１保持部１５０２から出力された、公開暗号鍵ＫＰｐ１と対になっている秘密復号鍵Ｋｐ１によって｛Ｋｓ２｝Ｋｐ１を復号し、セッションキーＫｓ２を暗号処理部１５０６へ出力する（ステップＳ２２０）。そうすると、セッションキー発生部１５０８は、再生セッション用のセッションキーＫｓ３を発生させ、

セッションキーＫｓ３を暗号処理部１５０６へ出力する（ステップＳ２２２）。暗号処理部１５０６は、セッションキー発生部１５０８からのセッションキーＫｓ３を復号処理部１５０４からのセッションキーＫｓ２によって暗号化して｛Ｋｓ３｝Ｋｓ２を出力し（ステップＳ２２４）、コントローラ１１０９は、バスＢＳ２およびメモリカードインタフェース１２００を介して｛Ｋｓ３｝Ｋｓ２をメモリカード１１０へ出力する（ステップＳ２２６）。

【０１４２】そうすると、メモリカード１１０の復号処理部１４１２は、端子１４２６、インタフェース１４２４、およびバスＢＳ４を介して｛Ｋｓ３｝Ｋｓ２を入力する。復号処理部１４１２は、セッションキー発生部１４１８によって発生されたセッションキーＫｓ２によって｛Ｋｓ３｝Ｋｓ２を復号して、再生端末１００で発生されたセッションキーＫｓ３を受理する（ステップＳ２２８）。

【０１４３】携帯電話機１００のコントローラ１１０９は、メモリカード１１０から事前に取得した再生リクエスト曲のライセンス管理ファイルからライセンスの格納されているエントリ番号を取得し（ステップＳ２３０）、メモリカードインタフェース１２００を介してメモリカード１１０へ取得したエントリ番号とライセンスの出力要求を出力する（ステップＳ２３２）。

【０１４４】メモリカード１１０のコントローラ１４２０は、エントリ番号とライセンスの出力要求とを受理し、エントリ番号によって指定された領域に格納されたライセンスを取得する（ステップＳ２３４）。

【０１４５】そして、コントローラ１４２０は、アクセス制限情報ＡＣｍを確認する（ステップＳ２３６）。

【０１４６】ステップＳ２３６においては、メモリのアクセスに対する制限に関する情報であるアクセス制限情報ＡＣｍを確認することにより、具体的には、再生回数を確認することにより、既に再生不可の状態である場合には再生動作を終了し、アクセス制限情報の再生回数に制限がある場合にはアクセス制限情報ＡＣｍの再生回数を変更した（ステップＳ２３８）後に次のステップ（ステップＳ２４０）に進む。一方、アクセス制限情報ＡＣｍの再生回数によって再生が制限されていない場合においては、ステップＳ２３８はスキップされ、アクセス制限情報ＡＣｍの再生回数は変更されることなく処理が次のステップ（ステップＳ２４０）に進行される。

【０１４７】ステップＳ２３６において、当該再生動作において再生が可能であると判断された場合には、メモリ１４１５のライセンス領域１４１５Ａに記録された再生リクエスト曲のライセンス鍵Ｋｃ１および再生制御情報ＡＣｐがバスＢＳ４上に出力される（ステップＳ２４０）。

【０１４８】得られたライセンス鍵Ｋｃと再生制御情報ＡＣｐは、切換スイッチ１４４６の接点Ｐｆを介して暗

号化処理部１４０６に送られる。暗号化処理部１４０６は、切換スイッチ１４４２の接点Ｐｂを介して復号処理部１４１２より受けたセッションキーＫｓ３によって切換スイッチ１４４６を介して受けたライセンス鍵Ｋｃ１と再生制御情報ＡＣｐとを暗号化し、｛Ｋｃ１／／ＡＣｐ｝Ｋｓ３をバスＢＳ４に出力する（ステップＳ２４０）。

【０１４９】バスＢＳ４に出力された暗号化データは、インタフェース１４２４、端子１４２６、およびメモリカードインタフェース１２００を介して再生端末１０２に送出される。

【０１５０】携帯電話機１００においては、メモリカードインタフェース１２００を介してバスＢＳ２に伝達される暗号化データ｛Ｋｃ／／ＡＣｐ｝Ｋｓ３を復号処理部１５１０によって復号処理を行ない、ライセンス鍵Ｋｃおよび再生制御情報ＡＣｐを受理する（ステップＳ２４２，Ｓ２４４）。復号処理部１５１０は、ライセンス鍵Ｋｃ（この場合はライセンス鍵Ｋｃ１）をスイッチ１５１１へ出力する。

【０１５１】また、復号処理部１５１０は、再生制御情報ＡＣｐをバスＢＳ２に出力する。コントローラ１１０９は、バスＢＳ２を介して、再生制御情報ＡＣｐを受理して再生の可否の確認を行なう（ステップＳ２４６）。

【０１５２】ステップＳ２４６においては、再生制御情報ＡＣｐによって再生不可と判断される場合には、端子１５１２にライセンス鍵Ｋｃｉを出力するようにスイッチ１５１１に指示し、Ｋｃ保持部１５１４はライセンス鍵Ｋｃｉを保持する。

【０１５３】このようにして、Ｋｃ保持部１４１５にライセンス鍵Ｋｃ１が保持され、「再生許諾」の処理が終了すると、暗号化コンテンツデータ｛Ｄｃ１｝Ｋｃ１が再生可能となる。一方、ステップＳ２１２，Ｓ２３６およびＳ２４６によって分岐し、Ｋｃ保持部１４１５にライセンス鍵Ｋｃ１が保持されないまま「再生許諾」が終了すると、暗号化コンテンツデータ｛Ｄｃ１｝Ｋｃ１が再生できない。

【０１５４】したがって、たとえ暗号化コンテンツデータ｛Ｄｃ｝Ｋｃの一部である試聴領域｛Ｄｃ１｝Ｋｃ１のみの再生であっても正規のライセンスを所持しないユーザが再生することはできない構成になっている。もちろん、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを何らかの手段で取得し、その取得した暗号化コンテンツデータ｛Ｄｃ｝Ｋｃをコピーしたものであってもよい。試聴用ライセンスを配信サーバ１０から取得すれば暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを再生可能である。

【０１５５】また、試聴においては試聴用ライセンスしか保持しないため、ライセンス鍵Ｋｃ２にて復号するように暗号化された試聴領域外のブロック、すなわち、本体領域｛Ｄｃ２｝Ｋｃ２は本体用ライセンスを取得しない限り、再生することはできない。

【０１５６】［本体用ライセンスの配信］次に、ステップＳ３０における本体用ライセンスのダウンロードについて詳細に説明する。本体用ライセンスのダウンロードは、試聴用ライセンスのダウンロードにおける処理と同様に、図１０および図１１のフローチャートに従って処理される。この場合、ライセンス鍵Ｋｃ２を含むライセンスのダウンロードであることから、ライセンス購入条件ＡＣには本体用ライセンスの購入であることを示す情報が含まれている。また、フローチャートにおけるライセンス鍵を区別する識別子ｉをｉ＝２、すなわちライセンス鍵ＫｃｉをＫｃ２に読替えればよく、説明が重複するので説明を省略する。

【０１５７】ここでは、本体用ライセンスを取得した後も、暗号化コンテンツデータの再生にはライセンス鍵Ｋｃ１を含む試聴用ライセンスを用いて再生するように説明したが、試聴用ライセンスにはアクセス制御情報ＡＣｍに含まれる再生回数制限を利用し、例えば、３回程度の回数制限を加えた上で、無償で配信し、本体用ライセンスとして２つのライセンス、すなわち、ライセンス鍵Ｋｃ１を含むライセンスとライセンス鍵Ｋｃ２を含むライセンスを同時に配信を行っても同様なサービスを提供することができる。この場合、携帯電話機１００は、図９のステップＳ３０において２つのライセンスの配信を受ける。つまり、図１０および図１１に示すフローチャートを２回処理することで取得することができる。

【０１５８】［再生］ステップＳ３０によって本体用ライセンスをダウンロードし、２つのライセンスをメモリカード１１０に格納した後に、２つのライセンス鍵Ｋｃ１，Ｋｃ２を用いて暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを再生する処理について説明する。ここでは、説明を簡単にするためにライセンス鍵Ｋｃ１はＫｃ保持部１５１４に、ライセンス鍵Ｋｃ２はライセンス保持部１５１５に保持されるものとして説明するが、これに限定されるものではなく逆であってもよい。

【０１５９】図３を参照して、暗号化コンテンツデータ９０を再生する場合について説明する。コントローラ１１０９は、暗号化コンテンツデータ９０に対する付加情報Ｄｃ－ｉｎｆを参照して、暗号化コンテンツデータ９０において試聴用領域９１に属するブロックと本体用領域９２に属するブロックを特定する。

【０１６０】次に、再生順序に従って最初のブロックを再生するために必要なライセンス鍵Ｋｃ２をＫｃ保持部１５１５に保持するための「再生許諾」を図１２のフローチャートに従って行なう。この場合、図１２のフローチャートにおけるライセンス鍵を区別する識別子ｉをｉ＝２、すなわちライセンス鍵ＫｃｉをＫｃ２に読替えればよく、試聴再生における「再生許諾」と同様であるため説明を省略する。

【０１６１】続いて、スイッチ１５１８に対して端子１５１７を選択して、Ｋｃ保持部１５１５に保持されてい

るライセンス鍵Ｋｃ２を出力するように指示し、暗号化コンテンツデータ９０を構成するブロックを再生順に従ってメモリカード１１０から読出して復号処理部１５１９に供給する。さらに、コントローラ１１０９は、暗号化コンテンツデータ９０を構成するブロックを、コンテンツデータの再生が連続して行なわれるように復号処理部１５１９に供給しつつ、その処理の空き時間を利用して、もう一つのライセンス鍵であるライセンス鍵Ｋｃ１をＫｃ保持部１５１４に保持させる「再生許諾」を試聴用領域９１に属するブロックの供給が開始される以前に行なう。ライセンス鍵Ｋｃ１に対する「再生許諾」は試聴における再生を行なう場合の「再生許諾」と同様であるので説明は省略する。

【０１６２】そうすると、コントローラ１１０９は、暗号化コンテンツデータ９０を構成するブロックをメモリカード１１０から読み出して、再生順に供給し、試聴用領域９１に達すると、スイッチ１５１８に対して端子１５１６を選択してＫｃ保持部１５１４に保持されているライセンス鍵Ｋｃ１を復号処理部１５１９に出力するよう指示し、引き続いて、暗号化コンテンツデータ９０を構成するブロックを再生順に従ってメモリカード１１０から読出して復号処理部１５１９に供給する。

【０１６３】そして、再び、本体用領域９２に達すると、再びスイッチ１５１８に対して端子１５１７を選択してＫｃ保持部１５１５に保持されているライセンス鍵Ｋｃ２を復号処理部１５１９に出力するよう指示し、引き続いて、暗号化コンテンツデータ９０を構成するブロックを再生順に従ってメモリカード１１０から読出して復号処理部１５１９に供給する。すべてのブロックが供給されると、暗号化コンテンツデータ９０の再生が終了する。

【０１６４】さらに、図３を参照して、暗号化コンテンツデータ９３を再生する場合について説明する。暗号化コンテンツデータ９３では、再生順に従うと、最初にライセンス鍵Ｋｃ１によって再生する試聴用領域９４が存在する。従って、まず、ライセンス鍵Ｋｃ１をＫｃ保持部１５１４に保持させる「再生許諾」を行なう。次いで、コントローラ１１０９は、暗号化コンテンツデータ９３を構成するブロックをメモリカード１１０から読み出して、再生順に復号処理部１５１９に供給する。さらに、コントローラ１１０９は、暗号化コンテンツデータ９３を構成するブロックを、コンテンツデータの再生が連続して行なわれるように復号処理部１５１９に供給しつつ、その処理の空き時間を利用して、もう一つのライセンス鍵であるライセンス鍵ｋｃ２をＫｃ保持部１５１５に保持させる「再生許諾」を本体用領域９５に属するブロックの供給が開始される以前に行なう。

【０１６５】本体用領域９５に達すると、スイッチ１５１８に対して、端子１５１７を選択してＫｃ保持部１５１４に保持されているライセンス鍵Ｋｃ２を復号処理部１５１９に出力するように指示し、引き続いて、暗号化コンテンツデータ９３を構成するブロックを再生順に従ってメモリカード１１０から読出して復号処理部１５１９に供給する。すべてのブロックが供給されると、暗号化コンテンツデータ９３の再生が終了する。

【０１６６】図１に示すパーソナルコンピュータ５０が配信サーバ１０またはＣＤ－ＲＯＭ６０から暗号化音楽データ｛Ｄｃ｝Ｋｃのみを取得して、カードライタ８０を介してメモリカード１１０に格納することもできる。この場合、図９のステップＳ１０における暗号化コンテンツデータのダウンロード処理が省略される。

【０１６７】また、図１に示すパーソナルコンピュータ５０は、試聴用の暗号化音楽データ｛Ｄｃ１｝Ｋｃ１、本体用の暗号化音楽データ｛Ｄｃ２｝Ｋｃ２、およびライセンス鍵Ｋｃ１を含む試聴用ライセンスを配信サーバ１０またはＣＤ－ＲＯＭ６０から取得して、カードライタ８０を介してメモリカード１１０に格納することができる。この場合、図９のステップＳ１０をパーソナルコンピュータ５０が行ない、パーソナルコンピュータ５０からカードライタ８０を介したメモリカード１１０へのライセンスの格納は、図１０および図１１に示すフローチャートに従って行なわれる。この場合、パーソナルコンピュータ５０は、図１０および図１１における配信サーバ１０と携帯電話機１００の機能を果たす。そして、携帯電話機１００のユーザは、カードライタ８０からメモリカード１１０を抜き、携帯電話機１００に装着し、図１２に示すフローチャートに従って暗号化音楽データ｛Ｄｃ｝Ｋｃの試聴領域｛Ｄｃ１｝Ｋｃ１を試聴する。その後、暗号化音楽データ｛Ｄｃ｝Ｋｃを聴きたいとき、携帯電話機１００によって配信サーバ１０から本体用の暗号化音楽データ｛Ｄｃ２｝Ｋｃ２を復号するためのライセンス鍵Ｋｃ２を図１０および図１１に示すフローチャートに従ってダウンロードする。そして、携帯電話機１００は、ユーザの再生要求に応じて、２つのライセンス鍵Ｋｃ１，Ｋｃ２を用いて暗号化音楽データ｛Ｄｃ｝Ｋｃの全てを再生する。また、説明をし省略したが、配信サーバ１０から試聴用ライセンスの取得、あるいはＣＤ－ＲＯＭ６０への試聴用ライセンスの記録および試聴用ライセンスの読出しは暗号技術を用いて安全性が確保されているものとする。ただし、ここでは、その方法については限定しないものとする。さらに、本体用ライセンスをコンピュータ５０にて配信サーバ１０から受信してカードライタ８０を介してメモリカード１１０に格納することも可能である。

【０１６８】このように、携帯電話機１００は、各種の経路から暗号化音楽データ｛Ｄｃ｝Ｋｃ、およびライセンス鍵Ｋｃ１，Ｋｃ２をそれぞれ含む２つのライセンスを受信してメモリカード１１０に記録する。したがって、携帯電話機１００のユーザが暗号化音楽データ｛Ｄｃ｝Ｋｃの全てを再生できる状態でのダウンロードを希

望したとき、メモリカード１１０には、最終的に、暗号化音楽データ｛Ｄｃ｝Ｋｃ、およびライセンス鍵Ｋｃ１，Ｋｃ２をそれぞれ含む２つのライセンスが格納される。

【０１６９】上記においては、暗号化コンテンツデータが音楽データを暗号化した暗号化コンテンツデータである場合について説明したが、暗号化コンテンツデータが他の朗読データ、教材データ、およびビデオデータ等であっても上述した方法によって暗号化コンテンツデータのダウンロード、試聴、試写および再生を行なう。

【０１７０】本発明の実施の形態によれば、複数のブロックに分割された暗号化コンテンツデータと、複数のブロックに含まれる暗号化データを復号するための複数のライセンスとを配信するので、各ブロックを異なるライセンスによって復号および再生できる。その結果、配信されるライセンスに応じて課金料金を設定できる。

【０１７１】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【０１７２】

【発明の効果】本発明によれば、複数のブロックに分割された暗号化コンテンツデータと、複数のブロックに含まれる暗号化データを復号するための複数のライセンスとを配信するので、各ブロックを異なるライセンスによって復号および再生できる。

【図面の簡単な説明】

【図１】　データ配信システムを概念的に説明する概略図である。

【図２】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図３】　暗号化コンテンツデータのフォーマットを示す図である。

【図４】　暗号化コンテンツデータの生成方法を説明するための図である。

【図５】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図６】　図１に示すデータ配信システムにおける配信サーバの構成を示す概略ブロック図である。

【図７】　図１に示すデータ配信システムにおける携帯電話機の構成を示す概略ブロック図である。

【図８】　図１に示すデータ配信システムにおけるメモリカードの構成を示す概略ブロック図である。

【図９】　図１に示すデータ配信システムにおける配信動作の全体構成を説明するためのフローチャートである。

【図１０】　図９に示すライセンスの配信動作をさらに詳細に説明するための第１のフローチャートである。

【図１１】　図９に示すライセンスの配信動作をさらに詳細に説明するための第２のフローチャートである。

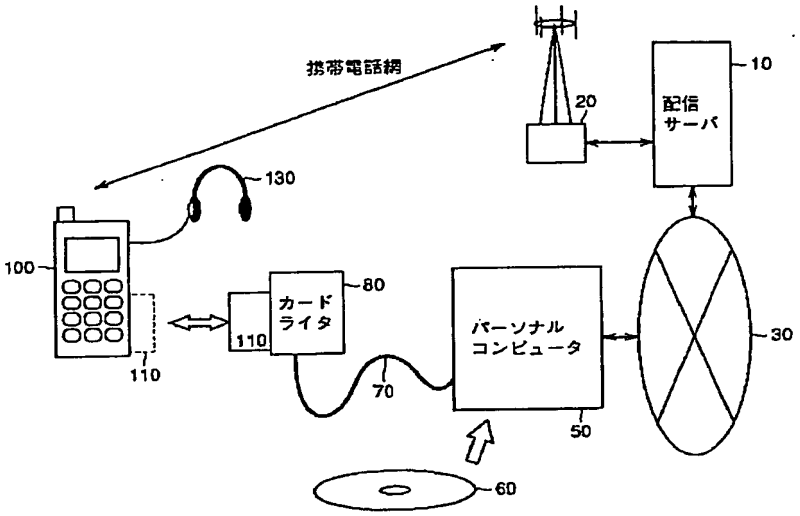
【図１２】　再生許諾動作におけるライセンス鍵の読出を詳細に説明するためのフローチャートである。

【図１３】　暗号化コンテンツデータの別のフォーマットを示す図である。

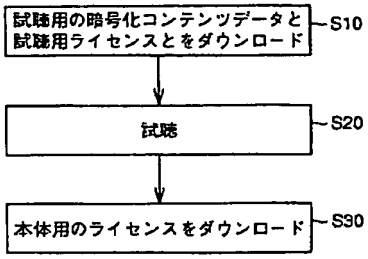
【符号の説明】

１０　配信サーバ、２０　配信キャリア、３０　インターネット網、５０　パーソナルコンピュータ、６０　ＣＤ、７０　ＵＳＢケーブル、８４，９０，９３，９６，９７　暗号化コンテンツデータ、８１　源データ、８２　ブロックデータ、８３，９１，９２，９４，９５，８４２，８４４，８４６　暗号化音楽データ１００　携帯電話機、１１０　メモリカード、１３０　ヘッドホーン、３０２課金データベース、３０４　情報データベース、３０７　メニューデータベース、３０８　配信記録データベース、３１０　データ処理部、３１２，３２０，１４０４，１４０８，１４１２，１４２２，１５０４，１５１０，１５１９　復号処理部、３１３　認証鍵保持部、３１５　配信制御部、３１６，１４１８，１５０８　セッションキー発生部、３１８，３２６，３２８，１４０６，１４１０，１４１７，１５０６　暗号処理部、３５０　通信装置、８４１，８４３，８４５，９７１，９７２　暗号化データ、９６１～９６７　領域、１１０９，１４２０コントローラ、１４２６，１５１２，１５１３，１５１６，１５１７，１５２２　端子、１１０１　アンテナ、１１０２　送受信部、１１０３　マイク、１１０４　ＡＤ変換器、１１０５　音声符号化部、１１０６　音楽再生部、１１０８スピーカ、１１１０　表示パネル、１１１１　操作パネル、１２００　メモリカードインタフェース、１４００，１５００　認証データ保持部、１４０２　Ｋｍｃ保持部、１４１４　ＫＰａ保持部、１４１５　メモリ、１４１５Ａ　ライセンス領域、１４１５Ｂ　データ領域、１４１６　ＫＰｍｃ保持部、１４２１　Ｋｍ保持部、１４２４　インタフェース、１４４２，１４４６　切換スイッチ、１５０２　Ｋｐ１保持部、１５２０　音楽再生部、１１０７，１５２１　ＤＡ変換器、１５１４，１５１５　Ｋｃ保持部、１５５０　コンテンツ再生回路。

【図１】



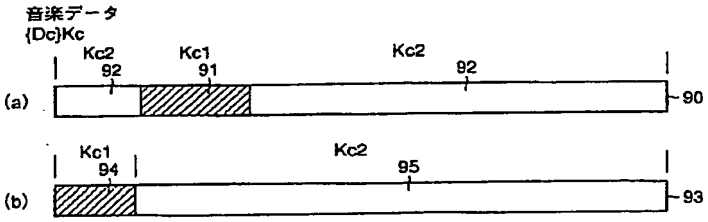
【図９】



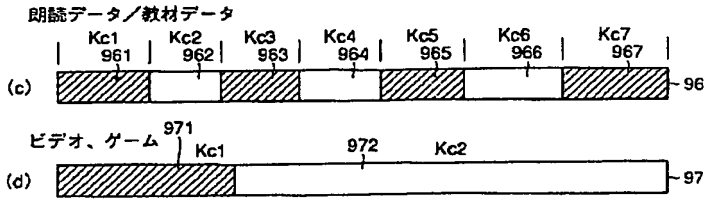
【図２】

記号	種類	属性	特性
Dc	コンテンツデータ	コンテンツ固有	例：音楽データ、朗読データ、教材データ、画像データ Kcにて復号可能な暗号化コンテンツデータ {Dc}Kcとして配信され、メモリカードに保持される
Dc-Inf	付加情報	コンテンツ固有	Dcに付随する平文データ。
Kc	ライセンス	コンテンツ固有	ライセンス 暗号化コンテンツデータを復号する復号鍵
ACm/ACp	ライセンス	ライセンス固有	制限情報 再生やライセンスの取り扱いに対する制限事項
ライセンスID	ライセンス	ライセンス固有	ライセンスを特定するための管理コード
コンテンツID	ライセンス	コンテンツ固有	コンテンツを特定するための管理コード
ライセンス	ライセンス	ライセンス固有	Kc＋ACm＋ACp＋ライセンスID＋コンテンツIDの総称

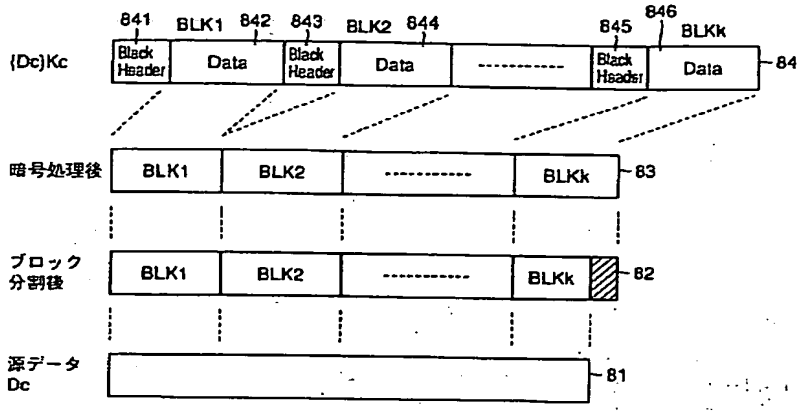
【図３】



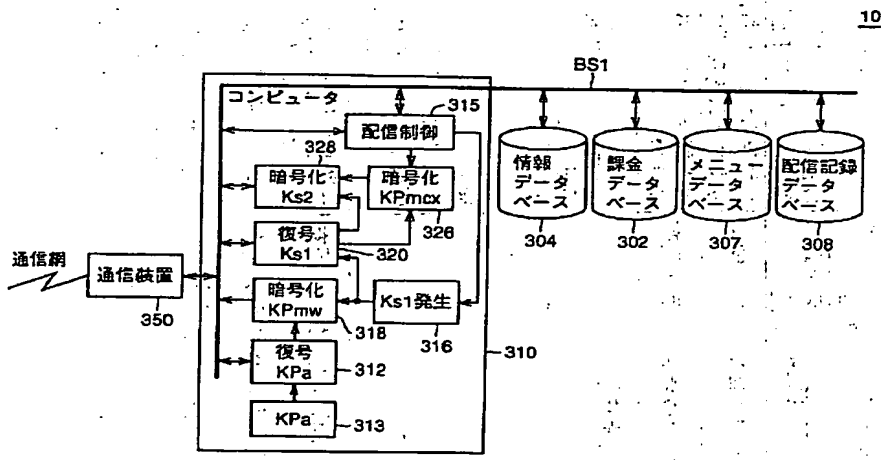
【図１３】



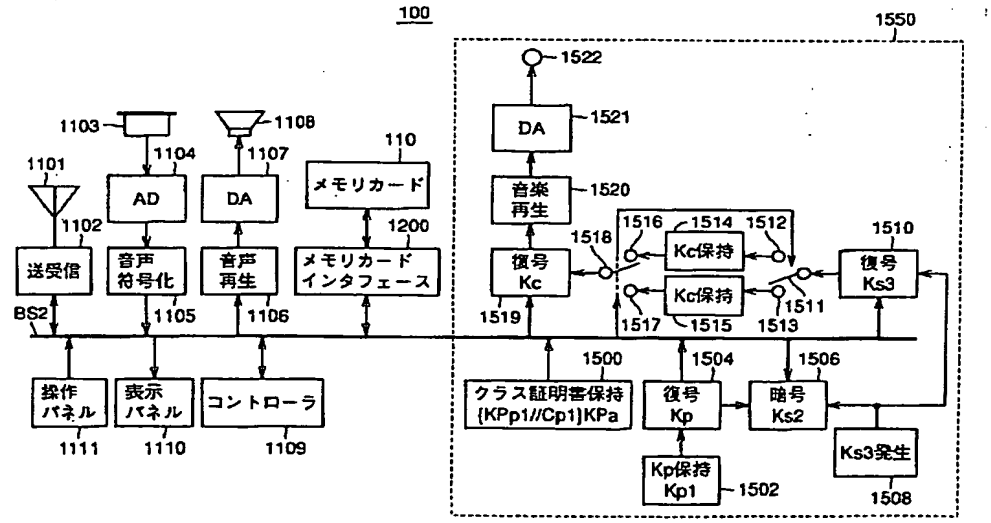
【図４】


841
BLK1
842
843
BLK2
844
845
846
BLKk
{Dc}Kc
Black Header
Data
Black Header
Data
Black Header
Data
84
暗号処理後
BLK1
BLK2
BLKk
83
ブロック分割後
BLK1
BLK2
BLKk
82
源データ Dc
81

【図６】


10
BS1
コンピュータ
315
配信制御
328
暗号化 Ks2
暗号化 KPmcx
326
復号 Ks1
320
暗号化 KPmw
318
Ks1発生
316
復号 KPa
312
KPa
313
310
情報データベース
304
課金データベース
302
メニューデータベース
307
配信記録データベース
308
通信網
通信装置
350

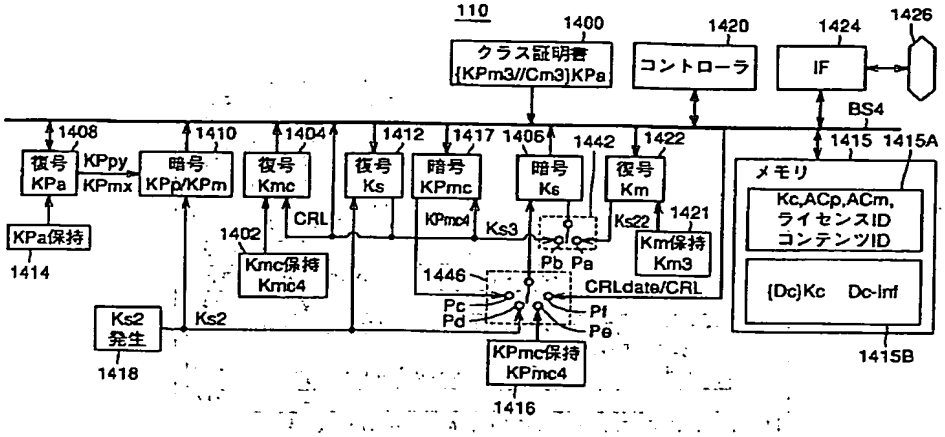
【図７】


100
1550
1103
1104
AD
1108
1107
DA
110
メモリカード
1101
1102
送受信
音声符号化
音声再生
1200
メモリカードインタフェース
BS2
1105
1106
操作パネル
表示パネル
コントローラ
1111
1110
1109
1522
DA
1521
音楽再生
1520
復号 Kc
1519
1516
1514
1512
1518
Kc保持
Kc保持
1517
1515
1513
1511
1510
復号 Ks3
1500
クラス証明書保持 {KPp1//Cp1}KPa
1504
復号 Kp
1506
暗号 Ks2
Ks3発生
1508
Kp保持 Kp1
1502

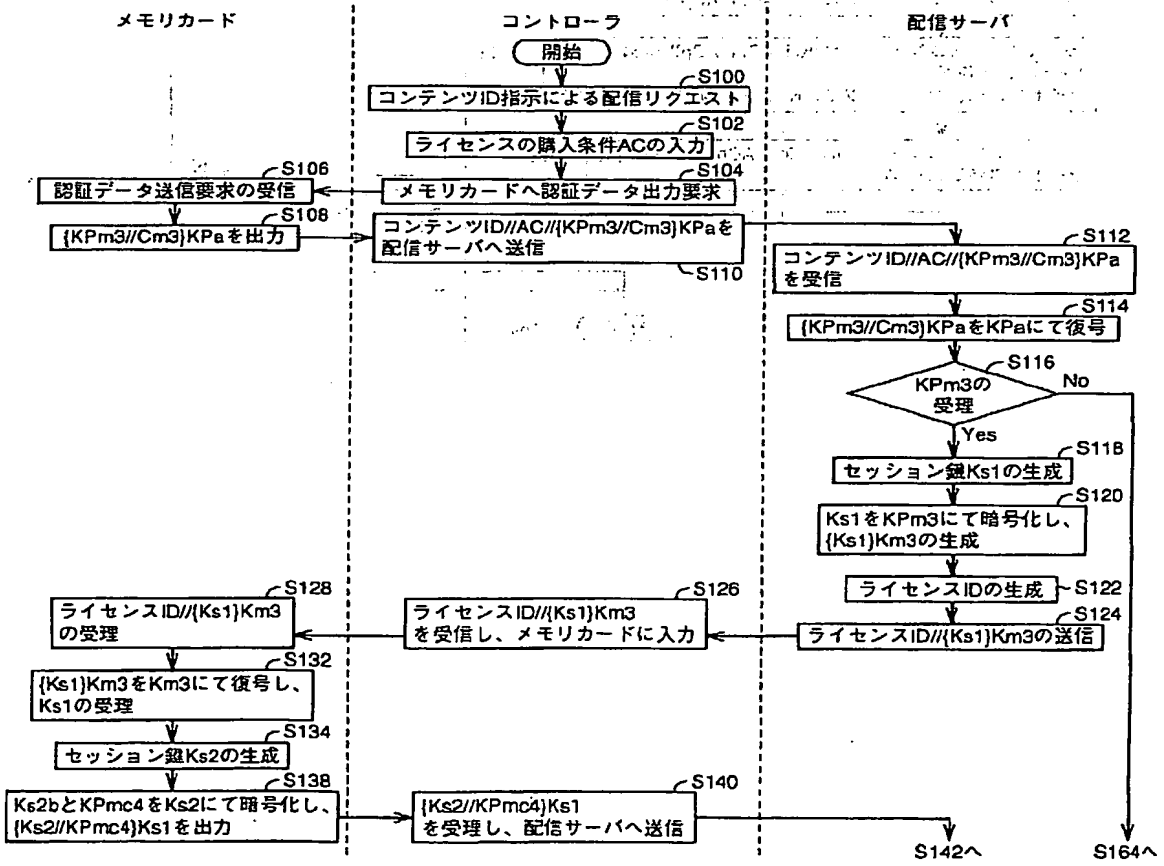
【図５】

	記号	種類	属性	特性
配信サーバ	KPa	公開認証鍵	システム共通	認証局にて認証データを復号する鍵
	Ks1	共通鍵	セッション固有	メモリカードへのライセンス配信ごとに発生
メモリカード	KPa	公開認証鍵	システム共通	認証局にて認証データを復号する鍵 配信サーバのKPaと同一
	KPmw	公開暗号鍵	クラス固有	証明書Cmwとともに認証局にて暗号化された認証データとして保持 wはクラスを識別するための識別子
	Kmw	秘密復号鍵	クラス固有	公開暗号鍵KPmwにて暗号化されたデータを復号する非対称な復号鍵
	KPmcx	公開暗号鍵	個別	メモリカードごとに異なる。 xはモジュールを識別するための識別子
	Kmcx	秘密復号鍵	個別	公開暗号鍵KPmcxにて暗号化されたデータを復号する非対称な復号鍵
	Ks2	共通鍵	セッション固有	配信サーバまたはコンテンツ再生回路間のライセンスの授受ごとに発生
	Cmw	証明書	クラス証明書	メモリカードのクラス証明書。認証機能を有する。 {KPmw//Cmw}KPaの形式で出荷時に記録。 ＊メモリカードのクラスwごとに異なる。
コンテンツ再生回路	KPpy	公開暗号鍵	クラス固有	証明書Cmwとともに認証局にて暗号化された認証データとして保持 yはクラスを識別するための識別子
	Kpy	秘密復号鍵	クラス固有	公開暗号鍵KPpyにて暗号化されたデータを復号する非対称な復号鍵
	Ks3	共通鍵	セッション固有	メモリカード間の再生セッションごとに発生
	Cpy	証明書	クラス証明書	コンテンツ再生デバイスのクラス証明書。認証機能を有する。 {KPpy//Cpy}KPaの形式で出荷時に記録。 ＊コンテンツ再生デバイスのクラスyごとに異なる。

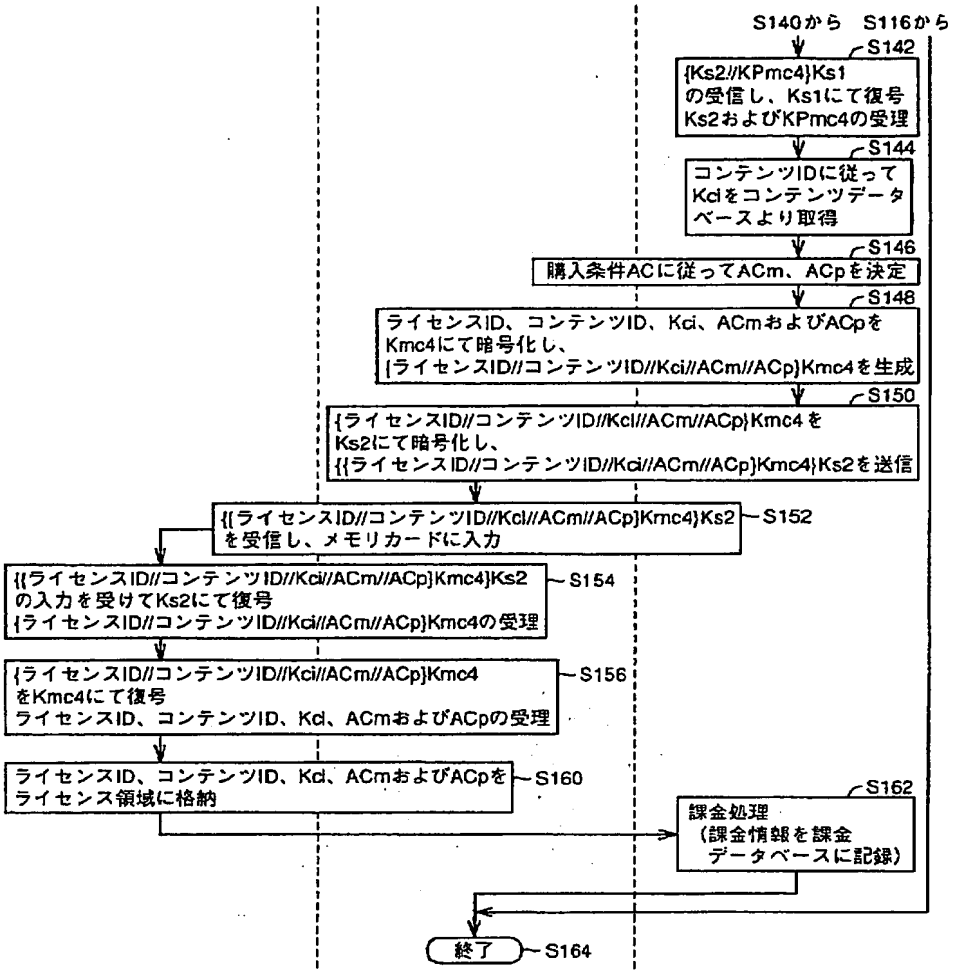
【図８】


110
1400
クラス証明書
{KPm3//Cm3}KPa
1420
コントローラ
1424
IF
1426
BS4
1408
復号
KPa
KPpy
KPmx
1410
暗号
KPp/KPm
1404
復号
Kmc
1412
復号
Ks
1417
暗号
KPmc
1406
暗号
Ks
1442
1422
復号
Km
1415
1415A
メモリ
Kc,ACp,ACm,
ライセンスID
コンテンツID
{Dc}Kc
Dc-Inf
1415B
KPa保持
1414
1402
Kmc保持
Kmc4
CRL
KPmc4
Ks3
Ks22
1421
Km保持
Km3
Pb
Pa
1446
CRLdate/CRL
Pc
Pd
Pf
Pe
Ks2
発生
1418
Ks2
KPmc保持
KPmc4
1416

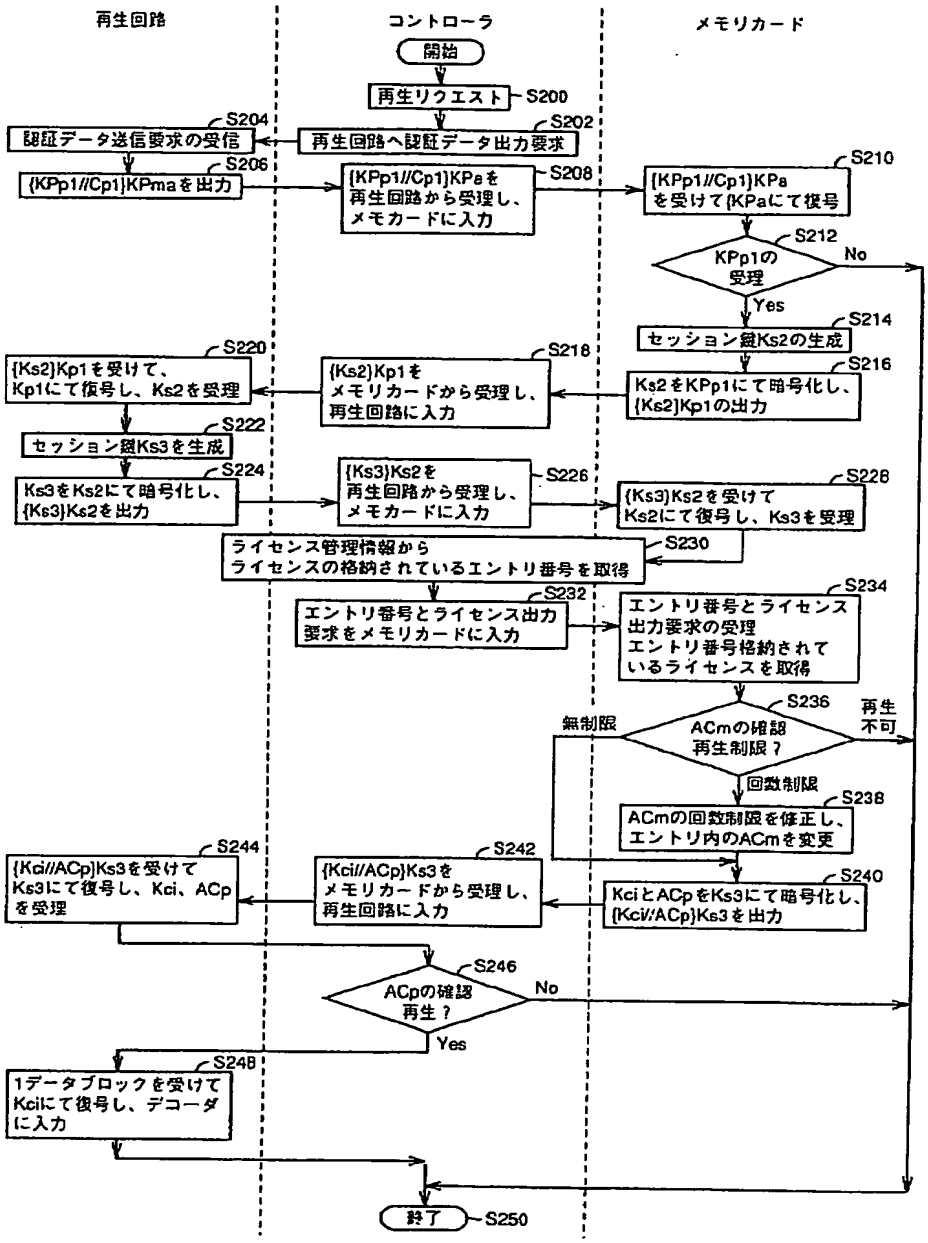
【図１０】


メモリカード
コントローラ
配信サーバ
開始
S100
コンテンツID指示による配信リクエスト
S102
ライセンスの購入条件ACの入力
S104
メモリカードへ認証データ出力要求
S106
認証データ送信要求の受信
S108
{KPm3//Cm3}KPaを出力
S110
コンテンツID//AC//{KPm3//Cm3}KPaを配信サーバへ送信
S112
コンテンツID//AC//{KPm3//Cm3}KPaを受信
S114
{KPm3//Cm3}KPaをKPaにて復号
S116
KPm3の受理
No
Yes
S118
セッション鍵Ks1の生成
S120
Ks1をKPm3にて暗号化し、{Ks1}Km3の生成
S122
ライセンスIDの生成
S124
ライセンスID//{Ks1}Km3の送信
S126
ライセンスID//{Ks1}Km3を受信し、メモリカードに入力
S128
ライセンスID//{Ks1}Km3の受理
S132
{Ks1}Km3をKm3にて復号し、Ks1の受理
S134
セッション鍵Ks2の生成
S138
Ks2bとKPmc4をKs2にて暗号化し、{Ks2//KPmc4}Ks1を出力
S140
{Ks2//KPmc4}Ks1を受理し、配信サーバへ送信
S142へ
S164へ

【図１１】


S140から　S116から
S142
{Ks2//KPmc4}Ks1
の受信し、Ks1にて復号
Ks2およびKPmc4の受理
S144
コンテンツIDに従って
Kciをコンテンツデータ
ベースより取得
S146
購入条件ACに従ってACm、ACpを決定
S148
ライセンスID、コンテンツID、Kci、ACmおよびACpを
Kmc4にて暗号化し、
{ライセンスID//コンテンツID//Kci//ACm//ACp}Kmc4を生成
S150
{ライセンスID//コンテンツID//Kci//ACm//ACp}Kmc4を
Ks2にて暗号化し、
{{ライセンスID//コンテンツID//Kci//ACm//ACp}Kmc4}Ks2を送信
{{ライセンスID//コンテンツID//Kci//ACm//ACp}Kmc4}Ks2
を受信し、メモリカードに入力
S152
{{ライセンスID//コンテンツID//Kci//ACm//ACp}Kmc4}Ks2
の入力を受けてKs2にて復号
{ライセンスID//コンテンツID//Kci//ACm//ACp}Kmc4の受理
S154
{ライセンスID//コンテンツID//Kci//ACm//ACp}Kmc4
をKmc4にて復号
ライセンスID、コンテンツID、Kci、ACmおよびACpの受理
S156
ライセンスID、コンテンツID、Kci、ACmおよびACpを
ライセンス領域に格納
S160
S162
課金処理
（課金情報を課金
データベースに記録）
終了
S164

【図１２】


再生回路
コントローラ
メモリカード
開始
再生リクエスト
S200
S202
再生回路へ認証データ出力要求
S204
認証データ送信要求の受信
S206
{KPp1//Cp1}KPmaを出力
{KPp1//Cp1}KPaを再生回路から受理し、メモカードに入力
S208
S210
{KPp1//Cp1}KPaを受けて{KPa}にて復号
S212
KPp1の受理
No
Yes
S214
セッション鍵Ks2の生成
S216
Ks2をKPp1にて暗号化し、{Ks2}Kp1の出力
S218
{Ks2}Kp1をメモリカードから受理し、再生回路に入力
S220
{Ks2}Kp1を受けて、Kp1にて復号し、Ks2を受理
S222
セッション鍵Ks3を生成
S224
Ks3をKs2にて暗号化し、{Ks3}Ks2を出力
{Ks3}Ks2を再生回路から受理し、メモカードに入力
S226
S228
{Ks3}Ks2を受けてKs2にて復号し、Ks3を受理
S230
ライセンス管理情報からライセンスの格納されているエントリ番号を取得
S232
エントリ番号とライセンス出力要求をメモリカードに入力
S234
エントリ番号とライセンス出力要求の受理
エントリ番号格納されているライセンスを取得
S236
ACmの確認
再生制限？
無制限
再生不可
回数制限
S238
ACmの回数制限を修正し、エントリ内のACmを変更
S240
KciとACpをKs3にて暗号化し、{Kci//ACp}Ks3を出力
S242
{Kci//ACp}Ks3をメモリカードから受理し、再生回路に入力
S244
{Kci//ACp}Ks3を受けてKs3にて復号し、Kci、ACpを受理
S246
ACpの確認
再生？
No
Yes
S248
1データブロックを受けてKciにて復号し、デコーダに入力
終了
S250